ALLOCATIONS OF PROBABILITY: A Theory of Partial Belief

Glenn Ray Shafer

A DISSERTATION

PRESENTED TO THE

FACULTY OF PRINCETON UNIVERSITY

IN CANDIDACY FOR THE DEGREE

OF DOCTOR OF PHILOSOPHY

RECOMMENDED FOR ACCEPTANCE BY THE

DEPARTMENT OF

STATISTICS

June, 1973

PREFACE

This essay constitutes Part II of a proposed monograph devoted to the exposition and justification of some of A.P. Dempster's methods of statistical inference. Part I of that monograph exists in draft form and is devoted primarily to a historical and critical account of the Bayesian paradigm for statistical inference. Statistical inference is not taken up directly in the present essay, but the ideas discussed here are directly relevant to a justification of Dempster's methods, some details of which may be found in my essay "A Theory of Statistical Support."

The ideas expounded here are directly inspired by my study of Professor Dempster's work, a study that began when I attended his seminar at Harvard in the spring of 1971. The reader will note that the quantities $Bel(A), P^*(A)$ treated axiomatically here correspond to the quantities $P_*(A), P^*(A)$ derived by Dempster from multivalued mappings. Unfortunately, the exact relationship between the present axiomatization and Dempster's original formulation remains somewhat obscure to me. In particular, I do not know how to express the condition of condensability in terms of multivalued mappings, though the examples that most interested Dempster were condensable.

The present essay does not include a discussion of the theory of integration on probability algebras. Using that theory, one can easily extend to allocations the discussion of several topics that are usually treated for distributions of probability. These include measures of location and dispersion, as well as analogues to entropy. Interestingly enough, the concept of entropy, rather overworked for distributions, breaks into two distinct concepts for allocations. One of these is related to the degree of conflict present in the evidence, while the other is related to the precision and strength of the evidence.

Aside from my obvious debt to Professor Dempster, I am also indebted to my wife Terry and my many other friends, teachers and fellow students who have helped me with these ideas. These include Paul Benacerraf, Thomas Corwin, Robert Epp, Alan Gross, Ian Hacking, Richard Hamming, Richard Jeffrey, Simon Kochen, Rod Montgomery, Edward Nelson, Dana Scott, Gary Simon, John Tukey and Paul Velleman. Peter Bloomfield, Richard Holley and Hale Trotter have been especially generous with their time. And Geoffrey Watson, my supervisor, has provided much needed encouragement.

I must also express my gratitude to the National Science Foundation; I have been supported by one of their graduate fellowships during the past three years.

ABSTRACT

A function Bel: $\mathcal{A} \to [0,1]$ on a Boolean algebra of propositions $\mathcal{A}$ is a belief function if

I. $Bel(\Lambda_{\mathcal{A}})=0$, where $\Lambda_{\mathcal{A}}$ is the impossible proposition.

II. $Bel(V_{\mathcal{A}})=1$, where $V_{\mathcal{A}}$ is the sure proposition.

III. $Bel(A_1 \vee \cdots \vee A_n) \geq \sum_i Bel(A_i) - \sum_{i<j} Bel(A_i \wedge A_j) + \cdots + (-1)^{n+1} Bel(A_1 \wedge \cdots \wedge A_n)$ for all $A_1, \ldots, A_n \in \mathcal{A}$.

The adoption of Bel means the adoption, for each $A \in \mathcal{A}$, of the quantity Bel(A) as one's degree of belief in the proposition A. If these degrees of belief correspond to the degrees to which the evidence supports the various A, then the quantities $P^*(A)=1-Bel(\bar{A})$ will correspond to the degrees to which the various A are plausible in light of the evidence.

Axioms I-III are satisfied by probability functions, but they are also satisfied by many functions that are not probability functions. In particular, they are always satisfied by the vacuous belief function, given by $Bel(V_{\mathcal{A}})=1$ and $Bel(A)=0$ for all $A \neq V_{\mathcal{A}}$.

A pair $(\mathcal{M}, \mu)$ is a probability algebra if $\mathcal{M}$ is a complete Boolean algebra and μ is a positive and completely additive measure with $\mu(V_{\mathcal{M}})=1$. A mapping ρ from a Boolean algebra of propositions $\mathcal{A}$ into a probability algebra $\mathcal{M}$ is called an allocation of probability if

1. $\rho(\Lambda_{\mathcal{A}})=\Lambda_{\mathcal{M}}$.
2. $\rho(V_{\mathcal{A}})=V_{\mathcal{M}}$.
3. $\rho(A \wedge B)=\rho(A) \wedge \rho(B)$ for all $A,B \in \mathcal{A}$.

As it turns out, $\mu \circ \rho$ is a belief function whenever ρ is an allocation of probability, and any belief function Bel: $\mathcal{A} \to [0,1]$ can be represented in the form $\mu \circ \rho$ for some allocation ρ on $\mathcal{A}$. Intuitively, the elements of $\mathcal{M}$ are probability masses, or portions of one's total belief, and $\rho(A)$ is that portion of one's belief which one commits to A. Hence the axioms for belief functions correspond to the idea that having a certain degree of belief in a proposition means committing that proportion of one's total belief to it.

An allocation ρ on a power set $\mathcal{P}(\mathcal{S})$ is <u>condensable</u> if $\rho(\bigcap \mathcal{C}) = \bigwedge_{C \in \mathcal{C}} \rho(C)$ for all $\mathcal{C} \subset \mathcal{P}(\mathcal{S})$. This is equivalent to $P^*(A) = \sup\{P^*(B) \mid B \subset A;\ B \text{ is finite}\}$ for all $A \subset \mathcal{S}$. Condensability can be defended as a natural condition for belief functions that are derived from empirical evidence, and it plays an important role in the abstract theory.

A belief function Bel_0 on a subalgebra $\mathcal{A}_0$ of a Boolean algebra $\mathcal{A}$ naturally induces a belief function Bel on $\mathcal{A}$. And belief functions on independent subalgebras of $\mathcal{A}$ can be combined by a natural rule to produce a belief function on $\mathcal{A}$. Study of this rule leads one to distinguish between <u>orthogonality</u> and <u>cognitive independence</u> for two independent subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ with respect to a belief function Bel. Orthogonality means that $\mathrm{Bel}(A \wedge B) = \mathrm{Bel}(A)\mathrm{Bel}(B)$ whenever $A \in \mathcal{A}_1$ and $B \in \mathcal{A}_2$, while cognitive independence means that $P^*(A \wedge B) = P^*(A)P^*(B)$ whenever $A \in \mathcal{A}_1$ and $B \in \mathcal{A}_2$.

Dempster's rules of conditioning and combination are techniques for modifying a belief function Bel: $\mathcal{A} \to [0,1]$ on the basis of new evidence or opinion. The rule of conditioning tells how to modify Bel when one learns that a given proposition $A \in \mathcal{A}$ is true. The rule of combination tells how to combine Bel with a new belief function Bel'$: \mathcal{Q} \rightarrow [0,1]$ so that the resulting belief function corresponds to the total evidence--the evidence that would be obtained by pooling the evidence underlying Bel with that underlying Bel'. Both of these rules are most applicable and most easily expressed in the condensable case.

TABLE OF CONTENTS

CHAPTER 1. DEGREES OF BELIEF

This chapter adduces and defends a set of rules governing degrees of belief for propositions in a Boolean algebra $\mathcal{Q}$.

Intuitively, a Boolean algebra of propositions $\mathcal{Q}$ is simply a collection of propositions which includes the impossible proposition Λ, the sure proposition V, the negation $\bar{A}$ of any of its elements A, and the conjunction $A \wedge B$ and the disjunction $A \vee B$ of any pair A,B of its elements. One writes $A \leq B$ to indicate that A implies B, and one assumes that A=B whenever both $A \leq B$ and $B \leq A$. I will assume that the reader is familiar with the mathematical structure of Boolean algebras and with the rules governing the symbols $\leq, \Lambda, V, -, \bar{\ }, \wedge$, and $\vee$. If he is not he may wish to consult Chapter 3 below, or he may wish to rely on a simple analogy with the symbols $\subset, \emptyset, \mathcal{S}, \sim, \tilde{\ }, \cap$ and $\cup$, as they apply to subsets of a set $\mathcal{S}$. ($A \subset B$ means that A is contained in B, $\emptyset$ denotes the empty set, $A \sim B$ is the set of points of A that are not in B, $\tilde{A} = \mathcal{S} \sim A$, $A \cap B$ denotes the intersection of the subsets A and B, and $A \cup B$ denotes the union of the subsets A and B.)

1. Axioms for Degrees of Belief

In Part I of this essay, I discussed at length reasons why the axiom of additivity is not always appropriate as a rule for degrees of belief, and I concluded in particular that it is not appropriate for the problem of statistical support. Nonetheless, I find that I cannot ignore the tremendous intuitive attraction of the classical theory of epistemic probability, and I can understand why many people find this attraction more weighty than any abstract argument. This attraction appears to stem from an intuitive understanding we have of probabilities, which, though it is seldom made entirely explicit, gives many of the rules that the subjective probabilist associates with degrees of belief a compelling, almost self-evident quality. We have an intuitive picture of probabilities, and it is that picture, rather than the formal rule of additivity, that we find hardest to give up.

The axiom of additivity is not, however, the most fundamental part of this intuitive picture. There are other rules that we associate with probabilities as degrees of belief that seem to be more fundamental, and correspondingly more self-evident. A good example is the rule of monotonicity, which states that if one proposition implies a second proposition, then the second proposition deserves at least as great a degree of belief as the first. In this chapter, we will discover that many of these more fundamental rules, as well as the intuitive picture underlying them, can be preserved even though the rule of additivity is dropped.

Let us take a closer look at the rule of monotonicity, for example, and try to understand the intuitive picture that makes it so self-evident. Denoting the degree of belief in A by Bel(A), we can express that rule by saying that

$$\text{if } A \leq B, \text{ then } \mathrm{Bel}(A) \leq \mathrm{Bel}(B).$$

Two corollaries of this rule are that Λ, the impossible proposition, should have the lowest degree of belief, conventionally zero, while V, the sure proposition, should have the highest degree of belief, conventionally one. The rule itself is obviously more than a convention; it is somehow necessary, given our intuitive ideas about how degrees of belief should work.

How can we make these intuitive ideas more explict? One way to bring them out is to examine the intuitive arguments that we might use in support of the rule of monotonicity. The reader is invited to consider what sort of intuitive argument he might offer; I find myself saying something like this: "If A implies B, then whenever A is true, B is true. So whatever belief I associate with A's being true, I must also associate with B's being true; and hence the belief I associate with B will <u>include</u> the belief I associate with A. In other words, the portion of my belief committed to B will include the portion committed to A. And in particular, its measure will be greater."

The fundamental feature of the picture revealed by this argument is that our belief appears in it as a measurable substance, various portions of which are committed to various propositions. This is natural enough an idealization; it merely makes explicit the notion that the relation between a degree of belief and complete belief is like the relation between a part and a whole. A secondary aspect of the picture is a restriction on our freedom in committing portions of this belief to various propositions, namely, the requirement that a portion of belief committed to a given proposition must also be committed to any more inclusive proposition. A further restriction, of course, is that none of our belief may be committed to Λ, while all of it must be committed to V; I accordingly adopt the convention that the total measure of our belief is equal to one.

What other restrictions are natural to this intuitive picture? One that seems natural enough is the requirement that a given portion of belief should not be simultaneously committed to two incompatible propositions. This requirement leads to the rule of superadditivity, which states that the degree of belief in the disjunction of two incompatible propositions should be at least as great as the sum of the degrees of belief for the separate propositions. In symbols:

$$\text{if } A \wedge B = \Lambda, \text{ then } \mathrm{Bel}(A) + \mathrm{Bel}(B) \leq \mathrm{Bel}(A \vee B).$$

In order to justify this rule, one should note that $A \leq A \vee B$ and $B \leq A \vee B$, so that the belief committed to $A \vee B$ must include both the belief committed to A and the belief committed to B. And there can be no overlap; since A and B are incompatible, none of the belief committed to one of them can also be committed to the other. Hence the measure of the belief committed to $A \vee B$ must be at least as great as the sum of the measures of these two separate portions of belief.

Notice that there is nothing in our intuitive picture to require that the inequality in the rule of superadditivity be replaced by equality. Equality would hold, evidently, only if all the belief committed to $A \vee B$ were necessarily committed either to A or to B. This would be a very strong restriction compared with the two restrictions that we have just considered, and we will find that it is not necessary for a coherent theory of degrees of belief.

This is not to say, though, that no further restrictions are appropriate on our freedom to commit our idealized portions of belief to different propositions. One further restriction that seems unavoidable is the requirement that any portion of belief that is committed to both of two propositions should also be committed to their logical conjunction. This may seem like a tautology, but it has a great many consequences.

For a start, we can use it to deduce the rule

$$\mathrm{Bel}(A)+\mathrm{Bel}(B)-\mathrm{Bel}(A\wedge B)\leq \mathrm{Bel}(A\vee B)$$

for all pairs of propositions in the Boolean algebra for which one has degrees of belief. The argument for this rule again depends on the fact that the belief committed to $A\vee B$ must include at least all the belief committed either to A or to B or to both. For the left-hand side represents the measure of this latter belief, obtained by adding the measure of the belief committed to A to the measure of the belief committed to B and subtracting the measure of what is counted twice, namely the belief committed both to A and to B.

A similar inequality will hold for triplets of propositions A, B and C:

$$\mathrm{Bel}(A)+\mathrm{Bel}(B)+\mathrm{Bel}(C)-\mathrm{Bel}(A\wedge B)-\mathrm{Bel}(A\wedge C)-\mathrm{Bel}(B\wedge C)+\mathrm{Bel}(A\vee B\vee C)\leq \mathrm{Bel}(A\vee B\vee C).$$

Here the left-hand side is the measure of all the belief that is committed to at least one of A, B and C. To see that this is so, notice that the quantity $\mathrm{Bel}(A)+\mathrm{Bel}(B)+\mathrm{Bel}(C)$ overstates that measure, for that portion of belief that is committed to both of any two of the propositions is counted twice, while that committed to all three is counted three times. When one subtracts the quantity $\mathrm{Bel}(A\wedge B)+\mathrm{Bel}(A\wedge C)+\mathrm{Bel}(B\wedge C)$, one is subtracting exactly once the measure of the belief committed to exactly two of the propositions, as is appropriate, but one is subtracting three times the measure of the belief committed to all three, and this is once too often. Hence one must finally add $\mathrm{Bel}(A\wedge B\wedge C)$ back again.

A similar inequality can be obtained for any finite collection $A_1,\ldots,A_n$ of propositions by comparing the measure of the belief committed to $A_1 \vee \cdots \vee A_n$ with the measure of all the belief that is committed to at least one of the A_i. That inequality is

$$\sum \mathrm{Bel}(A_i) - \sum \mathrm{Bel}(A_i \wedge A_j) + \sum \mathrm{Bel}(A_i \wedge A_j \wedge A_k) - + \cdots + (-1)^{n+1} \mathrm{Bel}(A_1 \wedge \cdots \wedge A_n) \leq \mathrm{Bel}(A_1 \vee \cdots \vee A_n$$

As we will see, these inequalities, together with the conventions $\mathrm{Bel}(\Lambda)=0$ and $\mathrm{Bel}(V)=1$, provide a satisfactory basis for a general theory of degrees of belief. Hence I will use them for a formal definition.

Definition. A function Bel on a Boolean algebra is a belief function if it takes values between zero and one and satisfies the following three axioms:

(I). $\mathrm{Bel}(\Lambda)=0$.

(II). $\mathrm{Bel}(V)=1$.

(III). If $n \geq 1$ and $A_1, \ldots, A_n$ are elements of the Boolean algebra, then

$$\mathrm{Bel}(A_1 \vee \cdots \vee A_n) \geq \sum \mathrm{Bel}(A_i) - \sum \mathrm{Bel}(A_i \wedge A_j) + - \cdots + (-1)^{n+1} \mathrm{Bel}(A_1 \wedge \cdots \wedge A_n).$$

My claim that this definition provides a satisfactory basis for a general theory of degrees of belief will be supported in two different ways in the following pages. On the one hand, we will see that these axioms more or less exhaust the consequences of our intuitive picture of "portions of belief" and that that intuitive picture is at least as attractive as the more special one usually associated with subjective probabilities. On the other hand, we will see that the axioms are general enough to encompass many systems of degrees of belief that are attractive and useful but fail to satisfy Kolmogorov's axioms. The demonstration that these new axioms are equivalent to the intuitive picture of portions of belief can be left for the next chapter, but it appropriate to illustrate their generality immediately.

2. Four Examples of Belief Functions

In this section I will exhibit four simple examples of belief functions. For the first two examples, I will verify Axiom III directly. For the last two, though, I will leave such a verification until the next chapter, where it will be facilitated by a fuller understanding of the structure of belief functions.

A. The Vacuous Belief Function

The simplest belief function on any Boolean algebra of propositions is the one that assigns degree of belief zero to every proposition except the sure proposition, which must of course have degree of belief one. This belief function corresponds to a complete lack of opinion—one has too little evidence or is too skeptical to assign a positive degree of belief to any proposition in the Boolean algebra except the one that is logically certain. I will call it the vacuous belief function. Axioms I and II obviously hold for this belief function, but how can we establish Axiom III?

First note that if none of the propositions $A_1,\ldots,A_n$ are equal to $\mathcal{V}$, then the right-hand side of the inequality is zero, so that the inequality necessarily holds. Suppose, on the other hand, that some of the A_i are equal to $\mathcal{V}$—say k of them. Then $\binom{k}{2}$ of the propositions $A_i \wedge A_j$ will also be equal to $\mathcal{V}$, $\binom{k}{3}$ of the propositions $A_i \wedge A_j \wedge A_k$, etc. Hence we will have

$$\sum \mathrm{Bel}(A_i)=k=\binom{k}{1},$$

$$\sum \mathrm{Bel}(A_i \wedge A_j)=\binom{k}{2},$$

$$\mathrm{Bel}(A_i \wedge A_j \wedge A_k)=\binom{k}{3},$$

etc., so that the right-hand side of the inequality will be

$$\binom{k}{1}-\binom{k}{2}+\binom{k}{3}-\cdots+(-1)^{k+1}\binom{k}{k}=1-(1-1)^k=1,$$

But $A_1 \vee \cdots \vee A_n$ will also be equal to V, so that the left-hand side, $Bel(A_1 \vee \cdots \vee A_n)$, will also be equal to 1, and the inequality will hold with equality. Hence Axiom III does indeed hold for the vacuous belief function.

B. Belief Functions on a Four-Element Boolean Algebra

The vacuous belief function is the only possible one on the two-element Boolean algebra $\{\Lambda, V\}$, but there are more possibilities for a four-element Boolean algebra $\{\Lambda, A, \bar{A}, V\}$. Suppose, for example that A is the proposition that there is life of Mars. A belief function on this Boolean algebra would then summarize one's degrees with respect to that proposition, both for and against it. Some might profess a complete lack of opinion about the proposition and adopt the vacuous belief function, but others will have some degree of belief either for or against it, or both, even if those degrees of belief are rather weak. One might, for example, profess a degree of belief of 1/10 in A, a degree of belief of 2/10 in $\bar{A}$, and of course a degree of belief 1 in $A \vee \bar{A} = V$. But will the function Bel with values $Bel(\Lambda)=0$, $Bel(A)=1/10$, $Bel(\bar{A})=2/10$ and $Bel(V)=1$ satisfy Axiom III?

It is not difficult to show that it does, as does any function $Bel: \{\Lambda, A, \bar{A}, V\} \rightarrow [0,1]$ that satisfies $Bel(\Lambda)=0$, $Bel(V)=1$ and $Bel(A)+Bel(\bar{A}) \leq 1$. Suppose, indeed, that $A_1, \ldots, A_n$ are all propositions from $\{\Lambda, A, \bar{A}, V\}$. Then let a be the number of the n propositions that are equal to Λ, b the number that are equal to A, c the number that are equal to $\bar{A}$, and d the number equal to V; $a+b+c+d=n$. Then

$$\sum Bel(A_i) = Bel(A)\binom{b}{1} + Bel(\bar{A})\binom{c}{1} + \binom{d}{1},$$

$$\sum \mathrm{Bel}(A_i \wedge A_j) = \mathrm{Bel}(A)\left[\binom{b}{2}+\binom{b}{1}\binom{d}{1}\right] + \mathrm{Bel}(\bar{A})\left[\binom{c}{2}+\binom{c}{1}\binom{d}{1}\right] + \binom{d}{2},$$

$$\sum \mathrm{Bel}(A_i \wedge A_j \wedge A_k) = \mathrm{Bel}(A)\left[\binom{b}{3}+\binom{b}{2}\binom{d}{1}+\binom{b}{1}\binom{d}{2}\right] + \mathrm{Bel}(\bar{A})\left[\binom{c}{3}+\binom{c}{2}\binom{d}{1}+\binom{c}{1}\binom{d}{2}\right] + \binom{d}{3},$$

etc.; and

$$\begin{aligned}
&\sum \mathrm{Bel}(A_i) - \sum \mathrm{Bel}(A_i \wedge A_j) + - \cdots + (-1)^{n+1}\mathrm{Bel}(A_1 \wedge \cdots \wedge A_n) \\
&= \mathrm{Bel}(A)\left[\binom{b}{1}-\binom{b}{2}+-\cdots+(-1)^{b+1}\binom{b}{b}\right]\left[\binom{d}{0}-\binom{d}{1}+-\cdots+(-1)^{d}\binom{d}{d}\right] \\
&+ \mathrm{Bel}(\bar{A})\left[\binom{c}{1}-\binom{c}{2}+-\cdots+(-1)^{c+1}\binom{c}{c}\right]\left[\binom{d}{0}-\binom{d}{1}+-\cdots+(-1)^{d}\binom{d}{d}\right] \\
&+ \left[\binom{d}{1}-\binom{d}{2}+-\cdots+(-1)^{d+1}\binom{d}{d}\right].
\end{aligned}$$

This last expression is equal to

	1	if $d>0$,
	$\mathrm{Bel}(A)+\mathrm{Bel}(\bar{A})$	if $d=0$, $c>0$, and $b>0$,
	$\mathrm{Bel}(A)$	if $d=0$, $c>0$, and $b=0$,
	$\mathrm{Bel}(\bar{A})$	if $d=0$, $c=0$, and $b>0$,
and	0	if $d=0$, $c=0$, and $b=0$.

But $\mathrm{Bel}(A_1 \vee \cdots \vee A_n)$ will be equal to

	1	if $d>0$,
	1	if $d=0$, $c>0$, and $b>0$,
	$\mathrm{Bel}(A)$	if $d=0$, $c>0$, and $b=0$,
	$\mathrm{Bel}(\bar{A})$	if $d=0$, $c=0$, and $b>0$,
and	0	if $d=0$, $c=0$, and $b=0$.

Hence Axiom III will indeed hold provided $\mathrm{Bel}(A)+\mathrm{Bel}(\bar{A}) \leq 1$. And it will not hold if $\mathrm{Bel}(A)+\mathrm{Bel}(\bar{A}) > 1$. Hence a function $\mathrm{Bel}: \{\Lambda, A, \bar{A}, \mathcal{V}\} \to [0,1]$ is a belief function if and only if it satisfies $\mathrm{Bel}(\Lambda)=0$, $\mathrm{Bel}(\mathcal{V})=1$ and $\mathrm{Bel}(A)+\mathrm{Bel}(\bar{A}) \leq 1$.

One consequence of this is that our notion of a belief function is general enough to accommodate degrees of belief arising from James

Bernoulli's notion of a "pure argument." (See Bernoulli's Artis Conjectandi, pp. 218-220; or Part I of this essay.) Indeed, Bernoulli obtained "probabilities" of β/α and zero, respectively, for a thing and its opposite when β out of $\alpha = \beta + \gamma$ cases proved the thing but the other γ cases proved nothing. If we translate "probability" into "degree of belief" and "thing and its opposite" into "proposition and its negation," this becomes $\mathrm{Bel}(A) = \beta/\alpha$ and $\mathrm{Bel}(\bar{A}) = 0$.

C. The Senate Example

A more picturesque example of a belief function involves the first meeting of the United States Senate in 1789. At the time of that meeting, eleven States had ratified the Constitution. Of these eleven, five chose Federalists to fill both of their Senate seats, four chose Democratic-Republicans, and two, Connecticut and Pennsylvania, chose both a Federalist and a Democratic-Republican. The overall split was thus twelve to ten in favor of the Federalists. The first order of business for the Senate was to select a temporary presiding officer who would have the honor of counting the ballots that elected George Washington as the first President of the United States. I do not know how that presiding officer was in fact selected, but let us imagine that in order to avoid State rivalry for such a historical honor, it was done by lot rather than by vote. Imagine, indeed, the following procedure: a soldier is employed to choose at random the name of a State and then select as he pleases one of the two Senators from that State. Examining this situation before the selection is made and having no knowledge about the preferences of the soldier, what reasonable degree of belief might I accord the proposition, say, that a Democratic-Republican will be chosen?

The phrase "at random" may raise questions in some minds, but for my purposes it suffices to suppose that the selection of the State is to be carried out in such a way that I am willing to accord a degree of belief of 1/11 to the proposition that any particular State will be chosen. On the other hand, by saying that the soldier selects one of the two Senators from the resulting State "as he pleases," and adding that I have no knowledge of his preferences, I mean to convey the notion that I have no positive degree of belief that he will choose one or the other.

The algebra of all the propositions about who will chosen corresponds in a natural way to the field of all subsets of the set of the twenty-two

Langdon	(D)	Wingate	(D)
Few	(D)	Gunn	(D)
Lee	(D)	Grayson	(D)
Izard	(D)	Butler	(D)
Johnson	(D)	Ellsworth	(F)
Maclay	(D)	Morris	(F)
Strong	(F)	Dalton	(F)
Paterson	(F)	Elmer	(F)
Bassett	(F)	Read	(F)
Carroll	(F)	Henry	(F)
King	(F)	Schuyler	(F)

The 22 Senators

New Hampshire	(D,D)
Georgia	(D,D)
Virginia	(D,D)
South Carolina	(D,D)
Connecticut	(D,F)
Pennsylvania	(D,F)
Massachusetts	(F,F)
New Jersey	(F,F)
Delaware	(F,F)
Maryland	(F,F)
New York	(F,F)

The 11 States

D	D
D	D
D	D
D	D
D	F
D	F
F	F
F	F
F	F
F	F
F	F

The 2 Parties

Figure 1. The Senate Problem

Senators. For example, the proposition that either Senator Carroll or Senator King will be chosen corresponds to the subset $\{$Carroll, King$\}$. The situation is illustrated by Figure 1. In the first panel of that figure, the set of Senators is shown; the second panel represents the same set, partitioned only to the extent of dividing the States; while in the third panel the set is partitioned between Democratic-Republican and Federalist Senators.

My degree of belief that a Democratic-Republican will be chosen seems to be 4/11, for I have that degree of belief that New Hampshire, Georgia, Virginia or South Carolina will be chosen, in which case the soldier cannot help choosing a Democratic-Republican. I cannot add any of the belief committed to Connecticut or Pennsylvania to this, for I do not claim any positive degree of belief that the soldier will choose the Democratic-Republican rather than the Federalist in the event that one of those States is chosen. Similarly, my degree of belief that a Federalist will be chosen is 5/11. And in general my degree of belief $Bel(A)$ that the Senator chosen will be in any given subset A of Senators will be $k/11$, where k is the number of States both of whose Senators are in A.

D. The Kansas Example

This final example is distinguished by the fact that the belief function is defined on an infinite Boolean algebra of propositions. Let us suppose that a military base is to be located somewhere in the State of Kansas, and that its exact location is to be determined as follows: One of the members of Congress from Kansas will be chosen at random, and he will be allowed to locate the base anywhere he pleases within the region he represents. Consider the Boolean algebra of all propositions of the form "The base will be located within R," where R is any region (or subset) of Kansas. What degrees of belief should one have for such propositions?

Well, there are seven Kansans in Congress; the five Representatives represent the districts shown in Figure 2, while each of the two Senators represent the State as a whole. Intuitively, our total belief must be divided into seven equal pieces, one corresponding to each of the seven politicians; and the degree of belief for the proposition "The base will be located in R" will be equal to k/7, where k is the number of districts which lie entirely within R. In particular, that degree of belief cannot exceed 5/7 unless R is the whole State, in which case the proposition is the sure proposition.

The collection $\mathcal{A}$ of all propositions of the form "The base will be located in R," where R is a subset of Kansas, is indeed a Boolean algebra. And it is infinite, for there are an infinite number of subsets of Kansas.

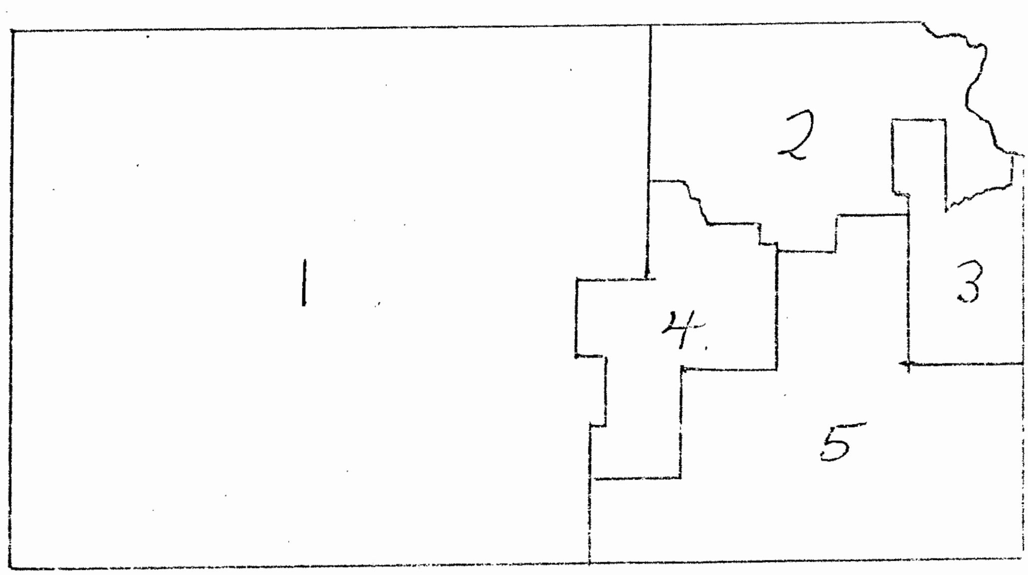

Figure 2. The Five Congressional Districts

And as we will see in the next chapter, the function

$$\text{Bel}: \mathcal{R} \rightarrow [0,1]: \text{"The base will be located in R."} \leadsto k/7,$$

where k is the number of districts lying entirely in R, is a belief function.

3. Upper Probabilities

The most striking feature of the preceding examples of degrees of belief is of course their failure to obey the rule of additivity, a failure that is most conspicuous in the case of a proposition and its negation. In practical terms, this failure of additivity means that one's degree of belief in a proposition does not necessarily determine one's degree of belief in its negation, so that the two quantities constitute distinct items of information. If degrees of belief were to follow the rule of additivity, then one's degree of belief $P(A)$ in a proposition A would determine one's degree of belief $P(\bar{A})$ in its negation through the relation $P(A)+P(\bar{A})=1$, or $P(\bar{A})=1-P(A)$; and once we knew someone's degree of belief in a proposition, we would learn nothing new if we were to be told his degree of belief in its negation. But the degrees of belief we have been studying do not work this way; we often have $\text{Bel}(A)+\text{Bel}(\bar{A}) < 1$, and knowledge of $\text{Bel}(A)$ does not guarantee knowledge of $\text{Bel}(\bar{A})$.

Another way of putting the matter is to say that a small value for $\text{Bel}(A)$ does not necessarily imply a large value for $\text{Bel}(\bar{A})$. Since $\text{Bel}(\bar{A})$ measures one's degree of belief in $\bar{A}$, or one's degree of disbelief in A, this assertion means, in English, that a low degree of belief does not necessarily imply a high degree of disbelief. In other words, we must distinguish between mere lack of belief and actual disbelief. Such a distinction is often left undrawn in everyday language: "I don't believe it" usually means "I believe the opposite." But it is a valuable distinction, and one that is usually made by careful thinkers. As an illustration of the distinction, consider again the proposition A="There is life on Mars," and its negation $\bar{A}$="There is no life on Mars." Suppose I know little about Mars, in particular have no reason to believe A, and accordingly have no belief in it whatever. Does this mean that I disbelieve A, i.e., that I have a strong belief in $\bar{A}$? I think not; it seems to me that an agnostic view is possible: I might entirely lack any belief either in A or $\bar{A}$. Or at less of an extreme, I might have no belief in A but only a mild belief in $\bar{A}$. For example, I might put $Bel(A)=0$ and $Bel(\bar{A})=\frac{1}{2}$.

A felicitous synonym for disbelief, as something susceptible of degree, is doubt, and this is the term I will employ in the sequel: one's degree of belief in $\bar{A}$ will be called one's degree of doubt for A. In this vocabulary, the assertion that both $Bel(A)$ and $Bel(\bar{A})$ might be small becomes the assertion that one might lack both belief and doubt for something. In many situations, one's degree of doubt for a proposition is more important than one's degree of belief in it. A low degree of doubt, for example, while not necessarily implying that one strongly believes a proposition, does indicate that one finds it plausible.

More generally, the extent to which one finds a proposition plausible is always inversely related to one's degree of doubt for it: the more one doubts it the less one finds it plausible. This fact leads us to think of the quantity $1-Bel(\bar{A})$ as a measure of the extent to which one finds A plausible. As it turns out, this quantity will play an important role in our theory, and it will be convenient to have a name for it. Following A. P. Dempster, I will call $1-\mathrm{Bel}(\overline{A})$ the <u>upper probability</u> of A, and denote it by $P^*(A)$.

The function $P^*: \mathcal{A} \rightarrow [0,1] : A \rightsquigarrow 1-\mathrm{Bel}(\overline{A})$ will be called the upper probability function associated with Bel. It obviously conveys exactly the same information as Bel does, for Bel can be recovered from P^* through the relation $\mathrm{Bel}(A)=1-P^*(\overline{A})$. What are the rules for P^* that correspond to our rules for Bel? This question is answered by the following definition and theorem:

<u>Definition</u>. A function $P^*: \mathcal{A} \rightarrow [0,1]$ on a Boolean algebra $\mathcal{A}$ is an <u>upper probability function</u> if

(1). $P^*(\Lambda)=0$.

(2). $P^*(V)=1$.

(3). If $n \geq 1$ and $A_1,\ldots,A_n$ are elements of $\mathcal{A}$, then

$$P^*(A_1 \wedge \cdots \wedge A_n) \leq \sum P^*(A_i) - \sum P^*(A_i \vee A_j) + - \cdots + (-1)^{n+1} P^*(A_1 \vee \cdots \vee A_n).$$

<u>Theorem</u>. A mapping $P^*: \mathcal{A} \rightarrow [0,1]$ is an upper probability function if and only if the mapping $\mathrm{Bel}: \mathcal{A} \rightarrow [0,1]$ defined by $\mathrm{Bel}(A)=1-P^*(\overline{A})$ is a belief function.

<u>Proof</u>: The only non-trivial part of the proof is the demonstration that the inequality (3) for P^* is equivalent to the third axiom for belief functions for Bel. Substituting $1-\mathrm{Bel}(\overline{A})$ for $P^*(A)$ in (3) gives

$$\begin{aligned} 1-\mathrm{Bel}(\overline{A}_1 \vee \cdots \vee \overline{A}_n) &\leq \sum [1-\mathrm{Bel}(\overline{A}_i)] - \sum [1-\mathrm{Bel}(\overline{A}_i \wedge \overline{A}_j)] + - \cdots + (-1)^{n+1} [1-\mathrm{Bel}(\overline{A}_1 \wedge \cdots \wedge \overline{A}_n \\ &= \left[\binom{n}{1} - \binom{n}{2} + - \cdots + (-1)^{n+1}\binom{n}{n}\right] \\ &\quad - \left[\sum \mathrm{Bel}(\overline{A}_i) - \sum \mathrm{Bel}(\overline{A}_i \wedge \overline{A}_j) + - \cdots + (-1)^{n+1} \mathrm{Bel}(\overline{A}_1 \wedge \cdots \wedge \overline{A}_n)\right]. \end{aligned}$$

Since $\binom{n}{1}-\binom{n}{2}+-\cdots+(-1)^{n+1}\binom{n}{n}=\binom{n}{0}-(1-1)^n=1$, this is equivalent to

$$\mathrm{Bel}(\bar{A}_1\vee\cdots\vee\bar{A}_n)\geq\sum\mathrm{Bel}(\bar{A}_i)-\sum\mathrm{Bel}(\bar{A}_i\wedge\bar{A}_j)+-\cdots+(-1)^{n+1}\mathrm{Bel}(\bar{A}_1\wedge\cdots\wedge\bar{A}_n).$$

Since (3) is equivalent to this last inequality for all $\bar{A}_1,\ldots,\bar{A}_n$ in $\mathcal{A}$, it is also equivalent to it for all $A_1,\ldots,A_n\in\mathcal{A}$, for every proposition in a Boolean algebra is the negation of some other proposition in it. But this gives us precisely the third axiom for belief functions. ▨

Rule (3) for upper probability functions can be written in another way which is also useful.

<u>Theorem.</u> Suppose f is a real-valued function on a Boolean algebra . Then f is an upper probability function if and only if

(i). $f(\Lambda)=0$.

(ii). $f(\mathrm{V})=1$.

(iii). If $n\geq 1$ and $B,A_1,\ldots,A_n$ are elements of $\mathcal{A}$, then

$$f(B)-\sum f(B\vee A_i)+\sum f(B\vee A_i\vee A_j)-+\cdots+(-1)^n f(B\vee A_1\vee\cdots\vee A_n)\leq 0.$$

<u>Proof:</u> Suppose indeed that f is an upper probability function. Then applying rule (3) to $B\vee A_1,\ldots,B\vee A_n$ yields

$$f(B\vee(\wedge A_i))\leq\sum f(B\vee A_i)-\sum f(B\vee A_i\vee A_j)+-\cdots+(-1)^{n+1}f(B\vee A_1\vee\cdots\vee A_n).$$

Since upper probability functions always take non-negative values, rule (3) implies in particular that f is monotone. Hence $f(B)\leq f(B\vee(\wedge A_i))$, and (iii) follows.

To see that (iii) implies rule (3) for upper probability functions, set $B=A_1\wedge\cdots\wedge A_n$ and transfer all the terms on the left-hand side of (iii) except the first to the right-hand side.

Finally, setting n=1 and choosing B and A_1 so that $B\leq A_1$, (iii) becomes $f(B)\leq f(A_1)$. Hence if f obeys (i)-(iii) it will take values between zero and one. Hence f [illegible]

The quantity

$$f(B)-\sum f(B\vee A_i)+\sum f(B\vee A_i\vee A_j)-+\cdots+(-1)^n f(B\vee A_1\vee\cdots\vee A_n)$$

can be written somewhat more compactly as

$$\sum_{J\subset\{1,\ldots,n\}} (-1)^{\text{card } J} f(B\vee(\bigvee_{i\in J} A_i)),$$

where card J, or the <u>cardinality</u> of J, is the number of elements in J, and $\bigvee_{i\in\emptyset} A_i$ is understood to be equal to Λ. It is sometimes denoted $\nabla_n^f(B;A_1,\ldots,A_n)$ and called the <u>n^{th}</u> <u>successive</u> <u>difference</u> of f(B) with respect to $A_1,\ldots,A_n$. This terminology derives from the fact that the quantities $\nabla_n^f(B;A_1,\ldots,A_n)$ can be specified recursively by the relations

$$\nabla_1^f(B;A_1)=f(B)-f(B\vee A_1)$$

and

$$\nabla_{n+1}^f(B;A_1,\ldots,A_{n+1})=\nabla_n^f(B;A_1,\ldots,A_n)-\nabla_n^f(B\vee A_{n+1};A_1,\ldots,A_n).$$

(See Choquet, p. 169.)

4. <u>The Logical and Subjective Vocabularies</u>

The theory that we have been developing in this chapter is overtly subjective. It is a theory of belief, and it deals with the degrees to which we believe and doubt propositions, not with the degrees to which they deserve belief or doubt. But the subjective notions of degree of belief and upper probability are obviously parallel to the logical notions of degree of support and degree of plausibility, developed in Part I of this essay. That parallelism, as exhibited in Table 1, connects belief with support and upper probability with plausibility.

The notions of support and plausibility are not subjective, for they refer to the objective relation between a proposition and the evidence for and against it; we take it as an objective, if sometimes elusive fact that the evidence does or does not support a proposition to a given degree, or that it does or does not leave it plausible to a given degree. But these logical quantities, if they are known, obviously determine the degrees of belief and the upper probabilities that we ought to have: we ought to believe a proposition to the extent that the evidence supports it, and our upper probability for a proposition, or the degree to which we find the proposition plausible, ought to equal its actual degree of plausibility.

My ultimate interest in this essay lies on the logical side of the ledger in Table 1; I want to measure degrees of support for statistical hypotheses. Why, then, am I constructing a subjective theory? The answer, of course, is that I will eventually want to impose on support functions the rules and structure that is being developed here for belief functions. Such an imposition will be partially justified by the general argument that degrees of support correspond to reasonable degrees of belief given the evidence and hence should obey rules that are appropriate for degrees of belief.

Subjective		Logical	
Degree of Belief	$Bel(A)$	Degree of Support	$S(A)$
Degree of Doubt	$Bel(\bar{A})$	Degree of Dubiety	$S(\bar{A})$
Upper Probability	$1-Bel(\bar{A})$	Degree of Plausibility	$1-S(\bar{A})$

Table 1. The Two Vocabularies

5. Probabilities as Degrees of Belief

The examples of Bernoulli and Lambert would provide some historical justification for the claim that degrees of belief satisfying our axioms for belief functions deserve to be called "probabilities," and I am tempted to make such a claim. But it is doubtful that such a claim would be accepted. Since the time of Laplace probabilities have had to be additive, and it seems likely that they will remain under that constraint for a good while.

A probability function on a Boolean algebra $\mathcal{A}$, then, is still a function $P: \mathcal{A} \to [0,1]$ that obeys the rules

(1). $P(\Lambda)=0$,

(2). $P(V)=1$,

and (3). $P(A)+P(B)=P(A\vee B)$ whenever $A,B \in \mathcal{A}$ and $A\wedge B=\Lambda$.

Since belief functions do not need to obey (3), they need not be probability functions. On the other hand, a probability function always qualifies as a belief function. To prove that this is so, it is only necessary to show that a probability function always obeys the inequalities in Axiom III for belief functions. Actually, a probability function always satisfies those inequalities with equality.

Theorem. If $P: \mathcal{A} \to [0,1]$ is a probability function and $A_1,\dots,A_n$ are any elements of $\mathcal{A}$, then

$$P(A_1\vee\cdots\vee A_n)=\sum P(A_i)-\sum P(A_i\wedge A_j)+-\cdots+(-1)^{n+1}P(A_1\wedge\cdots\wedge A_n).$$

Proof: Consider the set of all vectors $x=(x_1,\dots,x_n)$ such that each x_i is equal to either zero or one. For each such x, set $A_x=B_1\wedge\cdots\wedge B_n$, where $B_i=A_i$ if $x_i=1$ and $B_i=\overline{A}_i$ if $x_i=0$. Then all the A_x are in $\mathcal{Q}$, and they are pairwise incompatible. Further, $A_1\vee\cdots\vee A_n=\vee\{A_x \mid \text{some } x_i=1\}$ and $A_{i_1}\wedge\cdots\wedge A_{i_k}=\vee\{A_x \mid x_{i_1}=\cdots=x_{i_k}=1\}$. Thus

$$P(A_1\vee\cdots\vee A_n)=\sum\{P(A_x) \mid \text{some } x_i=1\},$$

and

$$\sum P(A_i)-\sum P(A_i\wedge A_j)+-\cdots+(-1)^{n+1}P(A_1\wedge\cdots\wedge A_n)$$
$$=\sum(\sum\{P(A_x) \mid x_i=1\})-\sum(\sum\{P(A_x) \mid x_i=x_j=1\})+-\cdots+(-1)^{n+1}P(A_1\wedge\cdots\wedge A_n).$$

The number of times that any particular x appears in this summation is evidently determined by the number of ones in x. In fact, if x contains r ones, then A_x will occur $\binom{r}{1}-\binom{r}{2}+-\cdots+(-1)^{r+1}\binom{r}{r}$ times. But this is equal to 1 unless r=0. Hence $P(A_x)$ occurs the same number of times in this formula as in the formula for $P(A_1\vee\cdots\vee A_n)$, and the equation is correct.

Obviously, a belief function is a probability function if and only if it obeys the axiom of additivity. More interesting, in light of the discussion in Part I, is the fact that a belief function is a probability function if and only if it obeys the special case of the axiom of additivity that relates the belief in a proposition to the belief in its negation. The proof of the non-trivial part of this assertion is given below:

<u>Theorem.</u> If a belief function Bel on a Boolean algebra $\mathcal{Q}$ satisfies $Bel(A)+Bel(\overline{A})=1$ for all $A\in\mathcal{Q}$, then Bel is a probability function.

<u>Proof:</u> We need to show that $Bel(A\vee B)=Bel(A)+Bel(B)$ for any two elements $A,B\in\mathcal{Q}$ such that $A\wedge B=\Lambda$. But we already know, by the rule of superadditivity, that $Bel(A\vee B)\geq Bel(A)+Bel(B)$, so we need

only show that $Bel(A \vee B) \leq Bel(A) + Bel(B)$. But if we apply Axiom III to $\overline{A}$ and $\overline{B}$, we obtain

$$Bel(\overline{A}) + Bel(\overline{B}) \leq Bel(\overline{A} \vee \overline{B}) + Bel(\overline{A} \wedge \overline{B}),$$

and substituting $1 - Bel(\overline{X})$ for $Bel(X)$ in each term of this inequality yields

$$1 - Bel(A) + 1 - Bel(B) \leq 1 - Bel(A \wedge B) + 1 - Bel(A \vee B).$$

Since $Bel(A \wedge B) = 0$, this becomes $Bel(A \vee B) \leq Bel(A) + Bel(B)$. ▨

So a belief function Bel is a probability function if and only if it satisfies $Bel(A) = 1 - Bel(\overline{A})$ for all A. But in general the upper probability function associated with a belief function Bel is given by $P^*(A) = 1 - Bel(\overline{A})$. So a belief function is a probability function if and only if it is identical to its upper probability function.

It is worth noting that the rule

$$P(A_1 \vee \cdots \vee A_n) = \sum P(A_i) - \sum P(A_i \wedge A_j) + - \cdots + (-1)^{n+1} P(A_1 \wedge \cdots \wedge A_n)$$

for probability functions also implies the rule

$$P(A_1 \wedge \cdots \wedge A_n) = \sum P(A_i) - \sum P(A_i \vee A_j) + - \cdots + (-1)^{n+1} P(A_1 \vee \cdots \vee A_n).$$

To derive the second equation from the first, one need only replace each A_i by $\overline{A}_i$. Hence probability functions also satisfy rule (3) for upper probability functions with equality.

From the point of view of our theory, then, a probability function is a special kind of belief function, and a "subjective probability" is a special kind of degree of belief. Indeed, it might be called a two-sided degree of belief, for it supplies a degree of belief both for a proposition and for the negation of that proposition.

6. Discounting Belief Functions

It often happens that we obtain our opinions and beliefs on a topic from someone else in whose judgment we have a reasonable degree of confidence. In most cases, of course, we will not have absolute confidence in this other person's opinions and hence will wish to discount those opinions at least slightly before adopting them as our own. This process of discounting can be represented quite simply in the theory of belief functions.

Suppose, indeed, that the other person's belief function is $Bel_0: \mathcal{Q} \to [0,1]$, and that one's degree of confidence in the other person's judgment is α, which is some number between zero and one. Then the natural thing to do is to adopt the quantity $\alpha \cdot Bel_0(A)$ as one's degree of belief in any proposition $A \in \mathcal{Q}$ that is not the sure proposition V. Formally, one would adopt the belief function $Bel: \mathcal{Q} \to [0,1]$ defined by $Bel(V)=1$ and $Bel(A)= \alpha \cdot Bel_0(A)$ for all $A \neq V$. It is easily verified that the function Bel defined in this way is indeed a belief function.

The process of discounting a belief function is a special case of the process of taking a linear mixture of two or more belief functions. If Bel_1 and Bel_2 are two different belief functions on the same Boolean algebra of propositions $\mathcal{Q}$, and if α is a number between zero and one, then the function $Bel: \mathcal{Q} \to [0,1]$ defined by $Bel(A)= \alpha\, Bel_1(A)+(1-\alpha)Bel_2(A)$ for all $A \in \mathcal{Q}$ will be a belief function; it is said to be a linear mixture of Bel_1 and Bel_2. It is evident that discounting a belief function Bel_0 by the factor α is the same as taking a linear mixture of Bel_1 and the vacuous belief function, using coefficients α and $(1-\alpha)$.

When a belief function is passed from person to person, being discounted each time, the degrees of belief accorded to the non-sure propositions constantly decrease. Hence the notion of discounting belief functions can be used to represent the diminishing credence that we lend to hearsay or to any tradition of testimony as its source becomes more remote.

These ideas are hardly novel. In fact, they were quite common in the eighteenth century discussions of the probability of testimony, which were much concerned with the bothersome idea that the probability of the scriptures diminishes with time. By and large, though, the notion of discounting "probabilities" did not survive into the nineteenth century. Its failure to survive can be attributed to its conflict with the rule of additivity for probabilities; for once additivity is assumed, the diminishing probability of the tradition comes to imply an increasing probability for the denial of the tradition--and this seems less reasonable.

7. A Counterexample

In Part I, I strongly criticized the attempt by some students of subjective probability to insist that "rational" degrees of belief ought to obey the rule of additivity. In fact, I questioned the very idea that abstract considerations could lead to rules that were absolutely obligatory for all reasonable systems of degrees of belief. But what about the rules that I have offered in this chapter? Are there reasonable systems of degrees of belief that would violate them?

There are, and it is easy to construct examples. One general method for constructing such examples is provided by the notion of an aleatory law. An aleatory law P on a set $\mathcal{X}$ is a function $P: \mathcal{P}(\mathcal{X}) \rightarrow [0,1]$, where $\mathcal{P}(\mathcal{X})$ is the set of all subsets of a set $\mathcal{X}$, and $P(A)$, for each $A \subset \mathcal{X}$, is taken to be the chance or objective probability that the outcome of a certain experiment or process will be in A. It is a commonplace that if we were really certain that some process were governed by an aleatory law then we would be justified in adopting as our degree of belief in the occurrence of a given event the chance assigned to that event by the aleatory law. The set $\mathcal{P}(\mathcal{X})$ can be interpreted, of course, as a Boolean algebra, and the resulting system of degrees of belief would be a probability function and hence a belief function. More generally, though, we might contemplate the situation, however fictional, in which we are absolutely certain that the process is governed by one of a given collection $\{P_\theta\}_{\theta \in \Theta}$ of aleatory laws. In such a case we might be justified in adopting as our degree of belief in the given event the infimum of the chances assigned that event by the various laws P_θ. More precisely, if the aleatory laws were on an observation space $\mathcal{X}$, we might define $B: \mathcal{P}(\mathcal{X}) \rightarrow [0,1]$ by $B(A) = \inf_{\theta \in \Theta} P_\theta(A)$. Such a function B will in general not be a probability function. And while it will satisfy $B(\emptyset)=0$ and $B(\mathcal{X})=1$, it will not satisfy Axiom III for belief functions unless the class of aleatory laws $\{P_\theta\}_{\theta \in \Theta}$ is chosen with particular care.

Dempster has given the following example where the function B does not satisfy Axiom III. Letting $\mathcal{X}$ consist of the four possibilities $\{bb, bw, wb, ww\}$, we contemplate the three aleatory laws given by

$$P_1(bb)=\tfrac{1}{4}, \quad P_1(bw)=\tfrac{1}{4}, \quad P_1(wb)=\tfrac{1}{4}, \quad P_1(ww)=\tfrac{1}{4};$$

$$P_2(bb)=\tfrac{1}{2}, \quad P_2(bw)=0, \quad P_2(wb)=\tfrac{1}{2}, \quad P_2(ww)=0;$$

$$P_3(bb)=0, \quad P_3(bw)=\tfrac{1}{2}, \quad P_3(wb)=0, \quad P_3(ww)=\tfrac{1}{2}.$$

We could imagine this situation arising if $\mathcal{X}$ consisted of all the possible results from drawing balls successively from two urns, the first of which was known to contain one black and one white ball, and the second of which might contain either one of each color or else two of the same color. The aleatory law P_1 would then correspond to the case where the second urn contained one black and one white ball, P_2 would correspond to the case where it contained two black balls, and P_3 to the case where it contained two white balls. Setting $A_1=\{bb, bw\}$ and $A_2=\{bb, ww\}$, we obtain $B(A_1)=B(A_2)=B(A_1 \vee A_2)=\frac{1}{2}$ and $B(A_1 \wedge A_2)=0$; and this violates the requirement that $B(A_1)+B(A_2)-B(A_1 \wedge A_2)$ should not exceed $B(A_1 \vee A_2)$.

8. Axiom III

In a sense, the third axiom for belief functions includes an infinite number of axioms, one for each natural number n. One might hope at first that it should be unnecessary to have so many axioms; perhaps the first few would imply the others. Unfortunately, though, it is necessary to state the axiom for an infinite number of different integers; for while the truth of the axiom for a given value of n implies its truth for smaller values, it does not imply its truth for larger values. This section is devoted to establishing these facts.

Theorem. Suppose $\mathcal{A}$ is a Boolean algebra, n is a natural number, and $B: \mathcal{A} \to [0,1]$ satisfies

(i). $B(\Lambda)=0$,

(ii). $B(V)=1$,

and (iii). $B(A_1 \vee \cdots \vee A_n) \geq \sum B(A_i) - \sum B(A_i \wedge A_j) + \cdots + (-1)^{n+1} B(A_1 \wedge \cdots \wedge A_n)$

for all sequences $A_1, \ldots, A_n$ of n elements of $\mathcal{A}$. Then

$$B(A_1\vee\cdots\vee A_{n-1})\geq\sum B(A_i)-\sum B(A_i\wedge A_j)+-\cdots+(-1)^n B(A_1\wedge\cdots\wedge A_{n-1})$$

for all sequences $A_1,\ldots,A_{n-1}$ of $n-1$ elements of $\mathcal{Q}$.

<u>Proof:</u> Suppose $A_1,\ldots,A_{n-1}$ are elements of $\mathcal{Q}$, and set $A_n=\Lambda$. Then by (iii),

$$B(A_1\vee\cdots\vee A_{n-1})=B(A_1\vee\cdots\vee A_n)\geq\sum_{i\leq n} B(A_i)-\sum_{i<j\leq n}B(A_i\wedge A_j)+-\cdots+(-1)^{n+1}B(A_1\wedge\cdots\wedge A_n)$$
$$=\sum_{i\leq n-1} B(A_i)-\sum_{i<j\leq n-1}B(A_i\wedge A_j)+-\cdots+(-1)^n B(A_1\wedge\cdots\wedge A_{n-1}).$$

<u>Theorem.</u> Let n be a natural number. Then there exists a Boolean algebra $\mathcal{Q}$ and a function $B:\mathcal{Q}\rightarrow[0,1]$ such that

(i). $B(\Lambda)=0$,

(ii). $B(V)=1$,

(iii). $B(S_1\vee\cdots\vee S_n)\geq\sum B(S_i)-\sum B(S_i\wedge S_j)+-\cdots+(-1)^{n+1}B(S_1\wedge\cdots\wedge S_n)$

for all sequences $S_1,\ldots,S_n$ of n elements of $\mathcal{Q}$, and yet

(iv). $B(A_1\vee\cdots\vee A_{n+1})<\sum B(A_i)-\sum B(A_i\wedge A_j)+-\cdots+(-1)^{n+2}B(A_1\wedge\cdots\wedge A_{n+1})$

for some sequence $A_1,\ldots,A_{n+1}$ of n+1 elements of $\mathcal{Q}$.

The rest of this section is devoted to an example establishing this theorem. Set $\mathcal{S}$ equal to a set of n+2 elements:

$$\mathcal{S}=\{a_1,\ldots,a_{n+2}\},$$

and set $\mathcal{Q}=\mathcal{P}(\mathcal{S})$, the set of all subsets of $\mathcal{S}$ interpreted as a Boolean algebra. Define $B:\mathcal{P}(\mathcal{S})\longrightarrow[0,1]$ by setting $B(A)$ equal to

	1	if $A=\mathcal{S}$,
	$2/(n+1)$	if A includes a_1 and n of $\{a_2,\ldots,a_{n+2}\}$,
	$1/(n+1)$	if A includes a_1 but fewer than n of $\{a_2,\ldots,a_{n+2}\}$,
and	0	if A does not include a_1.

Since $V=\mathcal{S}$ and $\Lambda=\emptyset$, conditions (i) and (ii) of the theorem are true for this example. The other two are also true, but more difficult to demonstrate.

First, let us establish (iv). To this end, note that a subset A of $\mathcal{S}$ satisfies $B(A)=2/(n+1)$ if and only if $A=\mathcal{S}-\{a_i\}$ for some i between 2 and n+1. Hence there are exactly n+1 distinct subsets of $\mathcal{S}$ that have a value of B equal to $2/(n+1)$. Denote these by $A_1,\ldots,A_{n+1}$. Then $B(A_1\vee\cdots\vee A_{n+1})=1$, while

$$\begin{aligned}&\sum B(A_i)-\sum B(A_i\wedge A_j)+\cdots+(-1)^{n+2}B(A_1\wedge\cdots\wedge A_{n+1})\\ &=\binom{n+1}{1}(2/(n+1))-\binom{n+1}{2}(1/(n+1))+\binom{n+1}{3}(1/(n+1))-+\cdots+(-1)^{n+2}\binom{n+1}{n+1}(1/(n+1))\\ &=1+(1/(n+1))\left[\binom{n+1}{1}-\binom{n+1}{2}+-\cdots+(-1)^{n+2}\binom{n+1}{n+1}\right]\\ &=1+(1/(n+1)).\end{aligned}$$

Hence (iv) is satisfied by the sequence $A_1,\ldots,A_{n+1}$.

Now let us establish (iii). Actually, we will establish that whenever $1\leq k\leq n$ and $S_1,\ldots,S_k$ are subsets of $\mathcal{S}$,

$$B(S_1\vee\cdots\vee S_k)\geq\sum B(S_i)-\sum B(S_i\wedge S_j)+-\cdots+(-1)^{k+1}B(S_1\wedge\cdots\wedge S_k). \qquad (1)$$

<u>Case 1</u>. $B(S_i)=2/(n+1)$ for $i=1,\ldots,k$. Let $A_1,\ldots,A_{n+1}$ be as above, and for each j, $j=1,\ldots,n+1$, let k_j be the number of the S_i equal to A_j. Then $k=k_1+\cdots+k_{n+1}$. And

$$B(S_i)=(2/(n+1))k=(1/(n+1))\left[\binom{k}{1}+\sum\binom{k_j}{1}\right],$$

$$B(S_i\wedge S_j)=(2/(n+1))\sum\binom{k_j}{2}+(1/(n+1))\left[\binom{k}{2}-\sum\binom{k_j}{2}\right]=(1/(n+1))\left[\binom{k}{2}+\sum\binom{k_j}{2}\right],$$

etc. Hence

$$\begin{aligned}&\sum B(S_i)-\sum B(S_i\wedge S_j)+-\cdots+(-1)^{k+1}B(S_1\wedge\cdots\wedge S_k)\\ &=(1/(n+1))\left[\binom{k}{1}-\binom{k}{2}+-\cdots+(-1)^{k+1}\binom{k}{k}\right]+(1/(n+1))\left[\sum\binom{k_j}{1}-\sum\binom{k_j}{2}+-\cdots+(-1)^{k+1}\sum\binom{k_j}{k}\right.\\ &=(r+1)/(n+1),\end{aligned}$$

where r is the number of j for which $k_j>0$, and $1\leq r\leq n$. If there is only one such j, then the above becomes $2/(n+1)$, which will be equal to $B(S_1\vee\cdots\vee S_k)=B(A_j)$. If there is more than one, then $B(S_1\vee\cdots\vee S_k)=1$, but $(r+1)/(n+1)$ will still not exceed 1, so (1) will still hold.

<u>Case 2</u>. Some of the S_i do not have $B(S_i)=2/(n+1)$. Let s be the number of the i, i=1,...,k, for which $B(S_i)\neq 2/(n+1)$. Then let us establish the inequality (1) by induction on s. The case s=0 was established in the preceding paragraph. So suppose $s \geq 1$, and suppose (1) holds for all smaller values of s. We may also assume that k is one of the i for which $B(S_i)\neq 2/(n+1)$. And the right-hand side of (1) becomes

$$\sum B(S_i)-\sum B(S_i \wedge S_j)+-\cdots+(-1)^{k+1}B(S_1\wedge\cdots\wedge S_k)$$

$$=B_1+B_2,$$

where

$$B_1=\sum_{i\leq k-1} B(S_i)-\sum_{i<j\leq k-1} B(S_i\wedge S_j)+-\cdots+(-1)^{k}B(S_1\wedge\cdots\wedge S_{k-1}),$$

and

$$B_2=B(S_k)-\Big(\sum_{i\leq k-1} B(S_k\wedge S_i)-\sum_{i<j\leq k-1} B(S_k\wedge S_i\wedge S_j)+-\cdots+(-1)^{k}B(S_k\wedge S_1\wedge\cdots\wedge S_{k-1})\Big).$$

By the inductive hypothesis, $B(S_1\vee\cdots\vee S_{k-1})\geq B_1$. Now consider separately the cases where $B(S_k)=1$ and where $B(S_k)$ is less than $2/(n+1)$. In the first case, $B(S_1\vee\cdots\vee S_k)=1$ and $B_2=1-B_1$, so $B(S_1\vee\cdots\vee S_k)=1=B_1+B_2$, and (1) holds. In the second case, $B_2=0$, and $B(S_1\vee\cdots\vee S_k)\geq B(S_1\vee\cdots\vee S_{k-1})\geq B_1=B_1+B_2$, and again (1) holds. This completes the demonstration.

9. <u>Bibliographic Notes</u>

Axiom III for belief functions was derived by A. P. Dempster for "lower probabilities induced by a multivariate mapping" in his 1967 paper in the <u>Annals of Mathematical Statistics</u>. Earler, Gustave Choquet had used Axiom III to define a "monotone set function of order ∞." (See pp. 169-71 of his "Theory of Capacities.") To my knowledge, though, no one has previously adduced these inequalities as intuitively appealing rules for degrees of belief.

The example involving the first United States Senate takes some liberties with history. Actually, only twelve of the twenty-two Senators were present on April 6, 1789, when the Senate elected John Langdon of New Hampshire as its President *pro tempore*. (See De Pauw, p. 8.) Furthermore, the division into the two parties was not clearly established at that time, so that the affiliations I have imputed to the various Senators are open to dispute. They are based on the votes of July 18, 1789, on the bill establishing a Department of Foreign Affairs, and the votes of August 4, 1789, on the bill establishing a Department of War. (De Pauw, pp. 86-7 and 104-6.)

For more information on the "non-additive probabilities" obtained by James Bernoulli and Johann Heinrich Lambert, the reader may consult pp. 218-220 of Bernoulli's *Artis Conjectandi* and pp. 318-421 of Volume 2 of Lambert's *Neues Organon*. Bernoulli's and Lambert's ideas are discussed in detail in Part I of this essay. References to the eighteenth century discussion of how the probability of testimony diminishes with its transmission can be found in Todhunter's history, pp. 54, 462 and 500. The matter was also discussed by Diderot in the article "Probabilité" of his famous *Encyclopédie*.

The example reproduced in section 7 was given on pp. 51-3 of Dempster's *The Theory of Statistical Inference*.

CHAPTER 2. ALLOCATIONS OF PROBABILITY

This chapter develops explicitly the intuitive picture underlying the axioms for belief functions. This results in the mathematical notion of an allocation of probability, and in the theorem that every belief function can be represented by an allocation of probability.

1. Constraint Relations

I used the term "portions of belief" in the preceding chapter so as to emphasize the differences between the theory developed there and probability theory, but it is evident that the intuition involved is really quite close to the intuition of students of subjective probability, who are accustomed to thinking of their probability as a measurable substance that can be divided into various pieces and distributed over a Boolean algebra of propositions. Indeed, it is in the method of distribution rather than in the nature of the abstracted probability that the differences will be found between the theory of belief functions and the more special theory of probability functions. Hence I find it entirely appropriate to follow the probabilist in using the word probability in place of the word belief when I am thinking of belief as something admitting of degree, and in the rest of this essay I will speak of pieces of probability or of probability masses rather than of portions of belief.

In this vocabulary, the intuitive picture developed in the preceding chapter involves the division of our probability into various probability masses, each of which may or may not be associated with or committed to a given proposition. There are of course restrictions on our freedom to commit probability masses to propositions; when I was adducing the rules for belief functions I mentioned the following ones:

(I) No probability mass may be committed to Λ.

(II) Every probability mass must be committed to V.

(III) If $A_1 \leq A_2$, then any probability mass committed to A_1 must also be committed to A_2.

(IV) Any probability mass that is committed to both A_1 and A_2 must also be committed to $A_1 \wedge A_2$.

This list is not exhaustive, though; we can easily extend it if we think a little more about the relations among our probability masses.

Our various probability masses are not conceived of in isolation; they are all pieces of the same fixed quantity of idealized substance representing our probability, and hence they can bear various relations to each other. For example, one probability mass may be part of another. Or one may consist precisely of the overlap between a pair of others, or perhaps of all the probability that is in either one or the other of a pair of others. I will write $M_1 \leq M_2$ to indicate that M_1 is part of M_2, or is contained in M_2; and I will denote by $M_1 \vee M_2$ the "union" of M_1 and M_2, or the probability mass consisting of all the probability that is in either M_1 or M_2.

Once we have established the ideas of containment and union for probability masses, the following additional rules impose themselves on the relation of "commitment" between probability masses and propositions:

(V) If the probability mass M_1 is committed to A and $M_2 \leq M_1$, then M_2 is also committed to A.

(VI) If the probability masses M_1 and M_2 are both committed to A, then the probability mass $M_1 \vee M_2$ is committed to A.

Evidently, the collection of our probability masses is beginning to acquire the same formal structure possessed by the collections of propositions we have dealt with; it is beginning to resemble a Boolean algebra.

In order to develop this structure further, let us denote the collection of our probability masses by the letter $\mathcal{M}$. We already have the relation "$\leq$" of containment which holds between some pairs of elements of $\mathcal{M}$; and for any two elements M_1, M_2, we have an element $M_1 \vee M_2$ which is their union. Intuitively, we should also have for each pair M_1, M_2 a probability mass $M_1 \wedge M_2 \epsilon \mathcal{M}$ representing their overlap or "intersection." And for each element $M \epsilon \mathcal{M}$ there ought to be an element $\overline{M} \epsilon \mathcal{M}$ which consists precisely of the probability that is not in M. There are difficulties, though, with the symbols "$\wedge$" and "$-$". The difficulty with writing $M_1 \wedge M_2$ is that M_1 and M_2 might be "disjoint" -- they might fail to overlap. In such a case there would be no probability mass for $M_1 \wedge M_2$ to denote. Similarly, if $M \epsilon \mathcal{M}$ is the probability mass consisting of all our probability, then there will be no probability left over to constitute the probability mass $\overline{M}$. Both of these problems can be met by the invention of a "null" probability mass, thought of as consisting of no probability at all. If we denote this null probability mass by Λ or $\Lambda_{\mathcal{M}}$ and denote the probability mass consisting of all our probability by V or $V_{\mathcal{M}}$, then we will be able to set $M_1 \wedge M_2 = \Lambda_{\mathcal{M}}$ whenever M_1 and M_2 do not overlap, and we will be able to set $\overline{V_{\mathcal{M}}} = \Lambda_{\mathcal{M}}$. It will also be convenient to establish the convention that $\Lambda_{\mathcal{M}} \leq M$ for all $M \epsilon \mathcal{M}$.

Our collection $\mathcal{M}$ of probability masses is now endowed with all symbols we have used for Boolean algebras of propositions. It has a relation "$\leq$", operations "$\wedge$", "$\vee$" and "$\bar{\ }$", and distinguished elements "Λ" and "V". Furthermore, these symbols have all the properties that we have been accustomed to in Boolean algebras of propositions. For example, $\Lambda \leq M \leq V$ for all $M \epsilon \mathcal{M}$; and for any $M \epsilon \mathcal{M}$, $M \wedge \overline{M} = \Lambda$ and $M \vee \overline{M} = V$. In the following pages I will call $\mathcal{M}$ a "Boolean algebra of probability masses" or a "probability algebra," and I will use these symbols and their properties freely.

In assuming that our probability is represented mathematically as a Boolean algebra $\mathcal{M}$, I am again taking for granted that the structure of Boolean algebras is intuitively clear. The reader who is dissatisfied with this intuitive approach may wish to turn to the first two sections of Chapter 3, where Boolean algebras are defined and studied abstractly.

We are dealing, then, with a Boolean algebra of probability masses $\mathcal{M}$ and a Boolean algebra of propositions $\mathcal{Q}$, and we have six rules that govern the relation of "commitment" between a probability mass $M \epsilon \mathcal{M}$ and a proposition $A \epsilon \mathcal{Q}$. If we write "M ct A" to signify that M is committed to A, these rules can be listed more neatly as follows:

(1) (a) If M ct A_1 and $A_1 \leq A_2$, then M ct A_2

(b) If M ct A_1 and M ct A_2, then M ct $A_1 \wedge A_2$.

(c) M ct $V_{\mathcal{Q}}$ for all $M \epsilon \mathcal{M}$.

(2) (a) If M_1 ct A and $M_2 \leq M_1$, then M_2 ct A.

(b) If M_1 ct A and M_2 ct A, then $M_1 \vee M_2$ ct A.

(c) $\Lambda_{\mathcal{M}}$ ct A for all $A \epsilon \mathcal{Q}$.

(3) If M ct $\Lambda_{\mathcal{Q}}$ then $M = \Lambda_{\mathcal{M}}$.

The last rule above, rule (3), has been slightly modified from its form as rule (I) in the first list; instead of saying that no probability mass can be committed to $\Lambda_{\mathfrak{A}}$, I now say that only the null probability mass can be so committed. And I have added a new rule, (2c), which says that the null probability mass is committed to any proposition. This is a harmless convention, and it rounds out the mathematical picture.

Both for reasons of euphony and for intuitive reasons that will emerge later, I will usually read "M ct A" as "M is constrained to A" rather than as "M is committed to A." And I will call a binary relation "ct" between a Boolean algebra of probability masses $\mathcal{M}$ and a Boolean algebra $\mathfrak{A}$ a <u>constraint relation</u> if it satisfies the three conditions just listed.

Thus far, I have argued that our collection $\mathcal{M}$ of probability masses should have the structure of a Boolean algebra, but it also has a further structure: every probability mass $M \in \mathcal{M}$ has a <u>measure</u>. We need, evidently, a function $\mu: \mathcal{M} \rightarrow [0, 1]$ that assigns to each element M its measure $\mu(M)$.

<u>Definition</u>. If $\mathcal{M}$ is a Boolean algebra, then a function $\mu: \mathcal{M} \rightarrow [0, 1]$ is a <u>measure</u> if

(1) $\mu(\Lambda_{\mathcal{M}}) = 0$,

(2) $\mu(V_{\mathcal{M}}) = 1$,

and (3) $\mu(M_1) + \mu(M_2) = \mu(M_1 \vee M_2)$ whenever $M_1, M_2 \in \mathcal{M}$ and $M_1 \wedge M_2 = \Lambda_{\mathcal{M}}$.

If $\mathcal{M}$ is a Boolean algebra and $\mu: \mathcal{M} \rightarrow [0, 1]$ is a measure, then the pair $(\mathcal{M}, \mu)$ is a <u>Boolean algebra of probability masses</u>, or a <u>measure algebra</u>.

Conditions (1) - (3) in this definition should be intuitively evident. Formally, they are the same conditions as those used in the previous chapter to define a "probability function" on a Boolean algebra. Hence a measure will have all the same properties as a probability function.

It may occur to the reader that the preceding definition of a measure algebra does not capture all the properties that we might intuitively ascribe to the idealized substance that represents our probability. The definition does not exclude, for example, the possibility that a probability mass M not equal to $\Lambda_{\mathcal{M}}$ might have $\mu(M) = 0$; yet intuitively a probability mass M ought always to have positive measure unless it contains no probability at all and hence is equal to $\Lambda_{\mathcal{M}}$. Another inadequacy of the present definition is the lack of any requirement of "additivity" for the measures of infinite disjoint collections of probability masses. Later we will find that we can impose further conditions on measure algebras so as to correct these inadequacies. The present definition, though, will serve us well in this chapter.

2. Allocations of Probability

The mathematical notion of a constraint relation still does not quite do full justice to the intuitive picture that I used to derive the axioms for degrees of belief in Chapter 1. For in that derivation I spoke repeatedly of the "total portion of belief associated with a given proposition." In the present vocabulary, this would be the total probability mass constrained to the proposition; and it is not clear how this "total probability mass" can be identified in terms of the constraint relation.

Intuitively, the "total probability mass" constrained to proposition $A \epsilon \mathcal{A}$ would be a probability mass $M \epsilon \mathcal{M}$ with the properties (i) M ct A and (ii) if $M' \epsilon \mathcal{M}$, then M' ct A if and only if $M' \leq M$. But unfortunately, nothing in our mathematical definition of a constraint relation requires the existence of such a probability mass M for each proposition A.

We need, then, to insist that such a probability mass $M \epsilon \mathcal{M}$ should exist for each $A \epsilon \mathcal{A}$. The natural way to do this is to postulate the existence of a mapping $\rho: \mathcal{A} \rightarrow \mathcal{M}$ that assigns the appropriate M to each A. The constraint relation ct can then be defined in terms of the mapping ρ.

What properties should the mapping ρ have? As it turns out, the essential properties of ρ are those determined by the facts that (i) No probability mass except $\Lambda_{\mathcal{M}}$ is constrained to $\Lambda_{\mathcal{A}}$, (ii) All the probability (i.e., $V_{\mathcal{M}}$) is constrained to $V_{\mathcal{A}}$, and (iii) The total probability mass constrained to $A_1 \wedge A_2$ consists precisely of the intersection of the total probability mass constrained to A_1 and the total probability mass constrained to A_2.

<u>Definition</u>. A mapping $\rho: \mathcal{A} \rightarrow \mathcal{M}$ from a Boolean algebra of propositions $\mathcal{A}$ to a Boolean algebra of probability masses $\mathcal{M}$ is an <u>allocation of probability</u> if ρ satisfies the following three conditions:

(i) $\rho(\Lambda_{\mathcal{A}}) = \Lambda_{\mathcal{M}}$,

(ii) $\rho(V_{\mathcal{A}}) = V_{\mathcal{M}}$,

(iii) $\rho(A_1 \wedge A_2) = \rho(A_1) \wedge \rho(A_2)$ for all $A_1, A_2 \epsilon \mathcal{A}$.

Since $\rho(A)$ is the total probability mass constrained to A, a given element $M \epsilon \mathcal{M}$ should be constrained to A if and only if $M \leq \rho(A)$. It is easily demonstrated that a binary relation defined in this way actually is a constraint relation. I will refer to it as the constraint relation given or specified by ρ.

<u>Theorem</u>. Suppose $\rho: \mathcal{A} \to \mathcal{M}$ is an allocation of probability. Then the binary relation "ct" between $\mathcal{M}$ and $\mathcal{A}$ defined by "M ct A if and only if $M \leq \rho(A)$" is a constraint relation.

<u>Proof</u>: It is necessary to establish conditions (1), (2) and (3) in the definition of a constraint relation. Condition (2) is immediate; and the others are implied by the three conditions in the definition of an allocation: (i) implies (3), (ii) implies (1c) and (iii) implies (1a) and (1b). ▨

It should be reiterated that not every constraint relation is specified by an allocation. But when there does exist an allocation specifying a given constraint relation, that allocation is unique.

Since $\rho(A)$ represents the total portion of our probability that is associated with the proposition A, its measure $\mu(\rho(A))$ ought to be our degree of belief in A. Hence the function $\mu \circ \rho: \mathcal{A} \to [1, 0]$ gives our degree of belief in the various propositions in $\mathcal{A}$. Will $\mu \circ \rho$ always be a belief function? It certainly ought to be, for the notion of an allocation of probability is a mathematical abstraction of the very intuitive picture that I used in deriving the axioms for belief functions.

<u>Theorem</u>. Suppose $(\mathcal{M}, \mu)$ is a Boolean algebra of probability masses, $\mathcal{A}$ is a Boolean algebra of propositions, and $\rho: \mathcal{A} \to \mathcal{M}$ is an allocation of probability. Then $\mu \circ \rho$ is a belief function on $\mathcal{A}$.

Proof: (i) $(\mu\circ\rho)(\Lambda_{\mathcal{Q}}) = \mu(\Lambda_{\mathcal{M}}) = 0.$

(ii) $(\mu\circ\rho)(V_{\mathcal{Q}}) = \mu(V_{\mathcal{M}}) = 1.$

(iii) Mathematically, the function μ qualifies as a probability function on $\mathcal{M}$. Hence, according to section 5 of the preceding chapter, μ itself satisfies the inequalities for belief functions with equality. And it is a simple consequence of the definition of an allocation (cf. Chapter 3, section 3) that $\rho(A_1) \leq \rho(A_2)$ whenever $A_1 \leq A_2$. Similarly, $\mu(M_1) \leq \mu(M_2)$ whenever $M_1 \leq M_2$. Hence for any elements $A_1, \ldots, A_n \in \mathcal{Q}$, $\rho(A_1) \vee \ldots \vee \rho(A_n) \leq \rho(A_1 \vee \ldots \vee A_n)$, and

$$\mu\circ\rho(A_1 \vee \ldots \vee A_n) \geq \mu(\rho(A_1) \vee \ldots \vee \rho(A_n))$$

$$= \sum_i \mu(\rho(A_i)) - \sum_{i<j} \mu(\rho(A_i)\wedge\rho(A_j)) + \ldots + (-1)^{n+1}\mu(\rho(A_1)\wedge\ldots\wedge\rho(A_n))$$

$$= \sum_i \mu\circ\rho(A_i) - \sum_{i<j} \mu\circ\rho(A_i\wedge A_j) + \ldots + (-1)^{n+1}\mu\circ\rho(A_1\wedge\ldots\wedge A_n).$$

Since it provides a mathematical representation for the intuitive picture underlying belief functions, the notion of an allocation of probability is the mathematical core of the theory of partial belief presented in this essay. In the bulk of this theory, the notion of an allocation will in fact be taken as basic. This seems to me to be appropriate, but it throws into question the adequacy of our axioms for degrees of belief. For it might be that some functions satisfying those axioms could not be represented by an allocation of probability. In fact, the axioms are adequate, and there are no such functions. In other words, if $\mathcal{Q}$ is a

Boolean algebra and Bel: $\mathcal{A} \to [0, 1]$ is a belief function, then there must exist a Boolean algebra of probability masses $(\mathcal{M}, \mu)$ and an allocation of probability $\rho: \mathcal{A} \to \mathcal{M}$ such that Bel $= \mu \circ \rho$. Most of the rest of this chapter is devoted to the proof of this fact.

3. Four Examples of Allocations

The simplest way to prove that a function Bel on a Boolean algebra $\mathcal{A}$ is a belief function is usually to construct an allocation that represents it. In this section I will provide such constructions for the examples of belief functions that were given in Chapter 1.

A. The Vacuous Belief Function

Recall that the vacuous belief function on a Boolean algebra $\mathcal{A}$ is given by

$$\mathrm{Bel}(A) = \begin{cases} 0 & \text{if } A \neq \mathbf{V}_{\mathcal{A}} \\ 1 & \text{if } A = \mathbf{V}_{\mathcal{A}}. \end{cases}$$

In order to represent this belief function, we construct a two-element measure algebra $\mathcal{M} = \{\Lambda_{\mathcal{M}}, \mathbf{V}_{\mathcal{M}}\}$, with $\mu(\Lambda_{\mathcal{M}}) = 0$ and $\mu(\mathbf{V}_{\mathcal{M}}) = 1$. We then define an allocation $\rho: \mathcal{A} \to \mathcal{M}$ by

$$\rho(A) = \begin{cases} \Lambda_{\mathcal{M}} & \text{if } A \neq \mathbf{V}_{\mathcal{A}} \\ \mathbf{V}_{\mathcal{M}} & \text{if } A = \mathbf{V}_{\mathcal{A}}. \end{cases}$$

It is easily verified that $(\mathcal{M}, \mu)$ is a measure algebra, that ρ is an allocation of probability, and that Bel $= \mu \circ \rho$. The construction can be described intuitively, of course, by saying that all one's probability is committed to $\mathcal{V}_{\mathcal{Q}}$, while none of one's probability is committed to any other proposition in $\mathcal{Q}$.

B. Belief Functions on a Four-Element Boolean Algebra

In Chapter 1, we saw that when $\mathcal{Q} = \{\Lambda, A, \overline{A}, \mathcal{V}\}$, any function $\text{Bel}:\mathcal{Q}\to[0, 1]$ satisfying $\text{Bel}(\Lambda) = 0$, $\text{Bel}(\mathcal{V}) = 1$ and $\text{Bel}(A) + \text{Bel}(\overline{A}) \leq 1$ is a belief function. In order to represent such a belief function, we require in general an eight-element measure algebra $\mathcal{M}$.

Suppose, indeed, that $\text{Bel}(A) = \alpha_1$ and $\text{Bel}(\overline{A}) = \alpha_2$; $\alpha_1 + \alpha_2 \leq 1$. Then we can construct $\mathcal{M}$ by postulating first that $\mathcal{M}$ contains disjoint probability mass M_1, M_2 and M_3 with measures α_1, α_2 and $1 - \alpha_1 - \alpha_2$ respectively, and then including all the unions of pairs of these three. More explicitly, say that $\mathcal{M}$ consists of:

$$
\begin{aligned}
&M_0 = \Lambda_{\mathcal{M}} && \text{with } \mu(M_0) = 0,\\
&M_1 && \text{with } \mu(M_1) = \alpha_1,\\
&M_2 && \text{with } \mu(M_2) = \alpha_2,\\
&M_3 && \text{with } \mu(M_3) = 1 - \alpha_1 - \alpha_2,\\
&M_4 = M_1 \vee M_2 && \text{with } \mu(M_4) = \alpha_1 + \alpha_2\\
&M_5 = M_1 \vee M_3 && \text{with } \mu(M_5) = 1 - \alpha_2\\
&M_6 = M_2 \vee M_3 && \text{with } \mu(M_6) = 1 - \alpha_1\\
&M_7 = M_1 \vee M_2 \vee M_3 = \mathcal{V}_{\mathcal{M}} && \text{with } \mu(M_7) = 1.
\end{aligned}
$$

Intuitively, $\mathcal{M}$ consists of all the probability masses that can be constructed from the three "basic probability masses," M_1, M_2 and M_3.

The allocation $\rho:\mathcal{Q}\to\mathcal{M}$ is given, of course, by $\rho(\Lambda_{\mathcal{Q}}) = \Lambda_{\mathcal{M}}$, $\rho(A) = M_1$, $\rho(\overline{A}) = M_2$, and $\rho(\mathcal{V}_{\mathcal{Q}}) = \mathcal{V}_{\mathcal{M}}$. Evidently, $\text{Bel} = \mu \circ \rho$.

C. The Senate Example

The measure algebra in this example is easy to describe intuitively: there are eleven disjoint basic probability masses, each with measure 1/11. It would be a bit tedious, though, to enumerate all the probability masses, for there are $2^{11} = 2,048$ of them.

Suppose we number the States shown in Figure 1 of Chapter 1 in the order they are shown there -- New Hampshire being number 1 and New York being number 11. Then we can suppose that our i'th basic probability mass, M_i, corresponds to the i'th State. The allocation $\rho: \mathcal{A} \rightarrow \mathcal{M}$ can then be described by saying that it maps the proposition A = "The Senator chosen will be in the subset A of the twenty-two Senators" into the probability mass formed by the union of all the basic probability masses corresponding to States both of whose Senators are in A. If there are k such states, the measure of $\rho(A)$ will be k/11.

D. The Kansas Example

For this example, we need six basic probability masses and $2^6 = 128$ probability masses in $\mathcal{M}$ altogether. Five of the basic probability masses, say, $M_1, \ldots, M_5$, have measure 1/7, while a sixth, say, M_6, has measure 2/7. The allocation $\rho: \mathcal{A} \rightarrow \mathcal{M}$ can be described by saying that $\rho(\mathbf{V}_{\mathcal{A}}) = \mathbf{V}_{\mathcal{M}} = M_1 \vee \ldots \vee M_6$, whereas if R is a proper subset of Kansas, ρ maps the proposition "The base will be located in R" into the probability mass consisting of the union of those probability masses M_i (i between one and five) such that the i'th Congressional district lies within R.

4. The Allowment of Probability

Let us pause to describe the upper probability function P^* in terms of the allocation ρ. Whereas Bel(A) can be understood as the measure of the total probability mass that is constrained to A, $P^*(A)$ can be understood as the measure of the total probability mass that is not constrained <u>away from</u> A. For $\rho(\bar{A})$ is the total probability mass that is constrained to $\bar{A}$, i.e., away from A; and its complement $\overline{\rho(\bar{A})}$ is therefore the total probability mass that is not constrained away from A. And $\mu(\overline{\rho(\bar{A})}) = 1 - \mu(\rho(\bar{A})) = 1 - \mathrm{Bel}(\bar{A}) = P^*(A)$.

Let $\zeta: \mathfrak{A} \to \mathfrak{M}$ be the mapping defined by $\zeta(A) = \overline{\rho(\bar{A})}$. Then $P^* = \mu \circ \zeta$. In the sequel we will often be interested in the upper probabilities of propositions and hence in the mapping ζ. Since $\zeta(A)$ can be described as the total probability mass that can be allowed to A, I will call ζ an <u>allowment</u>.

<u>Definition</u>. Suppose $\rho: \mathfrak{A} \to \mathfrak{M}$ is an allocation of probability. Then the mapping $\zeta: \mathfrak{A} \to \mathfrak{M} : A \rightsquigarrow \overline{\rho(\bar{A})}$ will be called the <u>allowment of probability corresponding to</u> ρ.

<u>Theorem</u>. Suppose $\zeta: \mathfrak{A} \to \mathfrak{M}$ is an allowment of probability. Then

(i) $\zeta(\Lambda_{\mathfrak{A}}) = \Lambda_{\mathfrak{M}}$.

(ii) $\zeta(V_{\mathfrak{A}}) = V_{\mathfrak{M}}$.

(iii) $\zeta(A_1 \vee A_2) = \zeta(A_1) \vee \zeta(A_2)$ for all $A_1, A_2 \in \mathfrak{A}$.

<u>Proof</u>. (i) $\zeta(\Lambda_{\mathfrak{A}}) = \overline{\rho(\overline{\Lambda_{\mathfrak{A}}})} = \overline{\rho(V_{\mathfrak{A}})} = \overline{V_{\mathfrak{M}}} = \Lambda_{\mathfrak{M}}$.

(ii) $\zeta(V_{\mathfrak{A}}) = \overline{\rho(\overline{V_{\mathfrak{A}}})} = \overline{\rho(\Lambda_{\mathfrak{A}})} = \overline{\Lambda_{\mathfrak{M}}} = V_{\mathfrak{M}}$.

(iii) $\zeta(A_1 \vee A_2) = \overline{\rho(\overline{A_1 \vee A_2})} = \overline{\rho(\bar{A}_1 \wedge \bar{A}_2)} = \overline{\rho(\bar{A}_1) \wedge \rho(\bar{A}_2)}$

$= \overline{\rho(\bar{A}_1)} \vee \overline{\rho(\bar{A}_2)} = \zeta(A_1) \vee \zeta(A_2)$. ▨

5. Some Simple Consequences of the Axioms

Our present task is to justify the claim that the axioms for degrees of belief actually force conformity with the intuitive picture involving allocations of probability. Our first step will be to explore some of the immediate consequences of those axioms.

First, let us verify that a belief function Bel: $\mathcal{A} \rightarrow [0, 1]$ does indeed obey the rule of monotonicity, i.e., that it satisfies $\mathrm{Bel}(A) \leq \mathrm{Bel}(B)$ whenever $A, B \in \mathcal{A}$ and $A \leq B$. To do so, we need only substitute A and B-A for A_1 and A_2 in axiom III for n = 2, obtaining

$$\mathrm{Bel}\,(A \vee (B-A)) \geq \mathrm{Bel}\,(A) + \mathrm{Bel}\,(B-A) - \mathrm{Bel}\,(A \wedge (B-A)),$$

or

$$\mathrm{Bel}(B) \geq \mathrm{Bel}(A) + \mathrm{Bel}(B-A).$$

Secondly, let us investigate in detail the quantities

$$\beta(A_1, \ldots, A_n) = \sum_i \mathrm{Bel}(A_i) - \sum_{i<j} \mathrm{Bel}(A_i \wedge A_j) + \ldots + (-1)^{n+1} \mathrm{Bel}(A_1 \wedge \ldots \wedge A_n)$$

for various collections $\{A_1, \ldots, A_n\}$ of elements of $\mathcal{A}$. Obviously, $\beta(A_1, \ldots, A_n)$ depends only on the collection $\{A_1, \ldots, A_n\}$, and not on the order of the A_i. According to our intuitive interpretation, $\beta(A_1, \ldots, A_n)$ should measure the total probability that is constrained to at least one of the A_i, and one can easily adduce many conditions that the quantities $\beta(A_1, \ldots, A_n)$ should satisfy if they are to conform to this intuitive interpretation. For example, they will have to satisfy

$$\beta(A_1, \ldots, A_n) \leq \beta(A_1, \ldots, A_{n+1}) \tag{1}$$

for all collections $\{A_1, \ldots, A_{n+1}\} \subset \mathcal{A}$.

Actually, (1) is easily deduced from the formula

$$\beta(A_1, \ldots, A_{n+1}) = \beta(A_1, \ldots, A_n) + \beta(A_{n+1}) - \beta(A_1 \wedge A_{n+1}, \ldots, A_n \wedge A_{n+1}), \tag{2}$$

which in turn follows from a simple calculation:

$$\begin{aligned}\beta(A_1, \ldots, A_{n+1}) &= \sum_i \mathrm{Bel}(A_i) - \sum_{i<j} \mathrm{Bel}(A_i \wedge A_j) + \sum_{i<j<k} \mathrm{Bel}(A_i \wedge A_j \wedge A_k) - + \ldots \\ &= \Big(\sum_{i\leq n} \mathrm{Bel}(A_i) - \sum_{i<j\leq n} \mathrm{Bel}(A_i \wedge A_j) + \sum_{i<j<k\leq n} \mathrm{Bel}(A_i \wedge A_j \wedge A_k) - + \ldots \Big) \\ &\quad + \Big(\mathrm{Bel}(A_{n+1}) - \sum_{i\leq n} \mathrm{Bel}(A_i \wedge A_{n+1}) + \sum_{i<j\leq n} \mathrm{Bel}(A_i \wedge A_j \wedge A_{n+1}) - + \ldots \Big) \\ &= \beta(A_1, \ldots, A_n) + \beta(A_{n+1}) - \beta(A_1 \wedge A_{n+1}, \ldots, A_n \wedge A_{n+1}).\end{aligned}$$

To deduce (1) from (2), we need only use the rule of monotonicity and axiom III to conclude that

$$\beta(A_{n+1}) = \mathrm{Bel}(A_{n+1}) \geq \mathrm{Bel}((A_1 \wedge A_{n+1}) \vee \ldots \vee (A_n \wedge A_{n+1})) \geq \beta(A_1 \wedge A_{n+1}, \ldots, A_n \wedge A_{n+1}).$$

Of course, formula (2) itself has a simple intuitive interpretation; it says that the measure of the probability constrained to one of the A_i, $i = 1, \ldots, n+1$, is equal to the measure of the probability constrained to one of the first n A_i plus the measure of the probability constrained to A_{n+1}, less the measure of that probability which is constrained to both A_{n+1} and one of the first n A_i and thus is counted twice.

If the element A_{n+1} were actually a subelement of one of the elements $A_1, \ldots, A_n$, say, $A_{n+1} \leq A_n$, then any probability constrained to A_{n+1} would already be constrained to A_n, and it would seem that equality should hold in (1). This is obviously true for $n = 1$, for if $A_2 \leq A_1$, then

$$\beta(A_1, A_2) = \text{Bel}(A_1) + \text{Bel}(A_2) - \text{Bel}(A_1 \wedge A_2)$$

$$= \text{Bel}(A_1) + \text{Bel}(A_2) - \text{Bel}(A_2)$$

$$= \beta(A_1).$$

And it follows for larger values of n by induction: if it is true for $n \leq k-1$, and $A_1, \ldots, A_{k+1} \in \mathcal{U}$ and $A_{k+1} \leq A_k$, then $A_i \wedge A_{k+1} \leq A_k \wedge A_{k+1}$ for $i = 1, \ldots, k$, and

$$\beta(A_{k+1}) = \beta(A_k \wedge A_{k+1}) = \beta(A_{k-1} \wedge A_{k+1}, A_k \wedge A_{k+1})$$

$$= \beta(A_{k-2} \wedge A_{k+1}, A_{k-1} \wedge A_{k+1}, A_k \wedge A_{k+1})$$

$$= \ldots = \beta(A_1 \wedge A_{k+1}, \ldots, A_k \wedge A_{k+1}),$$

and from (2) it follows that

$$\beta(A_1, \ldots, A_{k+1}) = \beta(A_1, \ldots, A_k).$$

It follows from (1) that whenever $\{A_1, \ldots, A_n\} \subset \{B_1, \ldots, B_m\} \subset \mathcal{Q}$, $\beta(A_1, \ldots, A_n) \leq \beta(B_1, \ldots, B_m)$. Actually this inequality will hold even when $\{A_1, \ldots, A_n\}$ is not contained in $\{B_1, \ldots, B_m\}$ provided that for each $A_i \in \{A_1, \ldots, A_n\}$ there is a $B_j \in \{B_1, \ldots, B_m\}$ such that $A_i \leq B_j$. For if the A_i are subelements of the B_j in this fashion, then it follows from the preceding paragraph that $\beta(B_1, \ldots, B_m) = \beta(B_1, \ldots, B_m, A_1, \ldots, A_n)$, and since $\{A_1, \ldots, A_n\} \subset \{B_1, \ldots, B_m, A_1, \ldots, A_n\}$, $\beta(A_1, \ldots, A_n) \leq \beta(B_1, \ldots, B_m, A_1, \ldots, A_n)$.

If two collections $\{A_1, \ldots, A_n\}$ and $\{B_1, \ldots, B_m\}$ are related in the fashion just described, i.e., if for each A_i there is a B_j such that

$A_i \leq B_j$, then it is convenient to say that $\{B_1, \ldots, B_m\}$ majorizes $\{A_1, \ldots, A_n\}$. In this vocabulary, the assertion of the preceding paragraph is simply that $\beta(A_1, \ldots, A_n) \leq \beta(B_1, \ldots, B_m)$ whenever $\{A_1, \ldots, A_n\}$ is majorized by $\{B_1, \ldots, B_m\}$. Similarly, $\beta(A_1, \ldots, A_n) = \beta(B_1, \ldots, B_m)$ whenever $\{A_1, \ldots, A_n\}$ and $\{B_1, \ldots, B_m\}$ majorize each other.

The following proposition may strike the reader as a bit too technical to provide any further insight into belief functions, but it will be useful to us later.

Theorem. Suppose $\{A_1, \ldots, A_n\}$, $\{B_1, \ldots, B_m\}$ and $\{C_1, \ldots, C_k\}$ are finite subsets of $\mathcal{Q}$. Suppose further that $\{B_1, \ldots, B_m\}$ majorizes $\{A_1, \ldots, A_n\}$, and that $\{A_1, \ldots, A_n\}$ majorizes $\{B_1 \wedge C_i, \ldots, B_m \wedge C_i\}$ for each i, i = 1, ..., k. Then

$$\beta(B_1, \ldots, B_m) - \beta(A_1, \ldots, A_n) = \beta(B_1, \ldots, B_m, C_1, \ldots, C_k) - \beta(A_1, \ldots, A_n, C_1, \ldots, C_k).$$

Proof. It suffices to prove the proposition for k = 1, i.e., for the case where $\{C_1, \ldots, C_k\} = \{C\}$. By (2),

$$\beta(B_1, \ldots, B_m, C) = \beta(B_1, \ldots, B_m) + \beta(C) - \beta(B_1 \wedge C, \ldots, B_m \wedge C),$$
$$\beta(A_1, \ldots, A_n, C) = \beta(A_1, \ldots, A_n) + \beta(C) - \beta(A_1 \wedge C, \ldots, A_n \wedge C).$$

Subtraction of the second equation from the first gives the desired result provided that

$$\beta(B_1 \wedge C, \ldots, B_m \wedge C) = \beta(A_1 \wedge C, \ldots, A_n \wedge C).$$

But this equation does hold, for it follows from the hypotheses of the theorem that $\{A_1 \wedge C, \ldots, A_n \wedge C\}$ and $\{B_1 \wedge C, \ldots, B_m \wedge C\}$ majorize each other. ▨

6. The Representation Theorem: Finite Case

Theorem. Suppose $\mathcal{Q}$ is a finite Boolean algebra and Bel: $\mathcal{Q} \to [0, 1]$ is a belief function. Then there exists a Boolean algebra of probability masses $(\mathcal{M}, \mu)$ and an allocation of probability $\rho: \mathcal{Q} \to \mathcal{M}$ such that Bel $= \mu \circ \rho$.

In order to prove this theorem, I will construct the measure algebra $\mathcal{M}$ as a field of subsets. (See Chapter 3, section 6) More precisely, I will take $\mathcal{M}$ to be the field of all subsets of $\mathcal{J} = \mathcal{Q} - \{\perp_{\mathcal{Q}}\}$, and define a constraint relation between $\mathcal{M}$ and $\mathcal{Q}$ by saying that M is constrained to A if and only if $A' \leq A$ for each $A' \in M$. This is indeed a constraint relation, and it is given by the allocation $\rho: \mathcal{Q} \to \mathcal{M}: A \rightsquigarrow \{A' \mid A' \leq A,\ A' \neq \perp_{\mathcal{Q}}\}$.

In order to define the measure μ on $\mathcal{M}$, first define the basic probability number m_A for each $A \in \mathcal{J}$ by

$$m_A = \text{Bel}(A) - \beta(A_1, \ldots, A_n),$$

where $A_1, \ldots, A_n$ are all the proper subelements of A, and β is defined as in section 5. The function μ is then defined by

$$\mu(M) = \sum_{A \in M} m_A .$$

Since the quantities m_A are non-negative, μ is evidently non-negative and additive; in order to show that μ is a measure on $\mathcal{M}$, it therefore suffices to show that $\mu(\mathcal{J}) = 1$. This, however, is merely a special case of the relation Bel(A) $= \mu(\rho(A))$, which we need to establish in general.

In order to verify that Bel(A) $= \mu(\rho(A))$, it is convenient to appeal to the fact that $\mathcal{Q}$ is isomorphic to the field of all subsets of the set $\mathcal{S}$ of atomic propositions of $\mathcal{Q}$. (See Chapter 3, section 6.) Thinking of each element A of $\mathcal{A}$ as a subset of $\mathcal{S}$, let c(A) denote its cardinality, and set $\mathrm{Par}(A) = (-1)^{c(A)}$. In other words, the <u>parity</u> of A is taken to be +1 if A has an even number of elements and -1 if A has an odd number of elements. Considering a fixed non-zero element A of $\mathcal{A}$, denote as before by $A_1, \ldots, A_n$ the proper subelements of A. Now, in general $n = 2^{c(A)} - 1$. Exactly c(A) of the elements $A_1, \ldots, A_n$, on the other hand, will obey $c(A_i) = c(A) - 1$; if we suppose that these are the first c(A), then $\{A_1, \ldots, A_n\}$ is majorized by $\{A_1, \ldots, A_{c(A)}\}$. Hence $\beta(A_1, \ldots, A_n) = \beta(A_1, \ldots, A_{c(A)})$. Now

$$\beta(A_1, \ldots, A_{c(A)}) = \sum_{i<c(A)} \mathrm{Bel}(A_i) - \sum_{i<j\leq c(A)} \mathrm{Bel}(A_i \cap A_j) + - \ldots + $$
$$+ (-1)^{c(A)+1} \mathrm{Bel}(A_1 \cap \ldots \cap A_{c(A)})$$

and it is easily seen that for each i, i = 1, ..., n $\mathrm{Bel}(A_i)$ occurs exactly once in the right-hand side of this equation, with sign equal to $\mathrm{Par}(A - A_i) = \mathrm{Par}(A) \cdot \mathrm{Par}(A_i)$. Hence

$$\beta(A_1, \ldots, A_{c(A)}) = -\mathrm{Par}(A) \sum_{A' < A,\, A' \neq A} \mathrm{Bel}(A')\, \mathrm{Par}(A'),$$

and

$$m_A = \mathrm{Bel}(A) - \beta(A_1, \ldots, A_{c(A)}) = \mathrm{Par}(A) \sum_{A' \leq A} \mathrm{Bel}(A')\, \mathrm{Par}(A').$$

With this expression for m_A, it is easy to verify that

$\mathrm{Bel}(A) = \mu(\rho(A))$: Setting $m_\Lambda = 0$, we can write

$$\mu(\rho(A)) = \mu(\{A' \mid A' \subset A,\ A' \neq \Lambda\})$$
$$= \sum_{A' \leq A,\ A' \neq \Lambda} m_{A'} = \sum_{A' \leq A} m_{A'}$$
$$= \sum_{A' \leq A} \mathrm{Par}(A') \Big(\sum_{A'' \leq A'} \mathrm{Bel}(A'')\, \mathrm{Par}(A'') \Big)$$

$$= \sum_{A'' \lesssim A} \mathrm{Bel}(A'')\,\mathrm{Par}(A'')\,\Big(\sum_{A'' \lesssim A' \lesssim A} \mathrm{Par}(A')\Big).$$

But

$$\sum_{A'' \lesssim A' \lesssim A} \mathrm{Par}(A') = (1-1)^{c(A'')-c(A)}\,\mathrm{Par}(A) = \begin{cases} 0 & \text{if } A \neq A'' \\ \mathrm{Par}(A) & \text{if } A = A'' \end{cases}$$

Hence

$$\mu(\rho(A)) = \mathrm{Bel}(A).$$

7. Measures on Semifields of Subsets

In order to prove our representation theorem in the general case, we need to know how to extend a measure from a semifield to a field of subsets. The exposition in this section is adapted from Kolmogorov and Fomin, pp. 17-22.

Definition. A non-empty collection $\mathcal{E}$ of subsets of a non-empty set $\mathcal{S}$ is called a semifield of subsets of $\mathcal{S}$ if it satisfies the following conditions:

(i) $\mathcal{E}$ contains the empty set ϕ.

(ii) $\mathcal{E}$ contains the set $\mathcal{S}$ itself.

(iii) If $A, B \in \mathcal{E}$, then $A \cap B \in \mathcal{E}$.

(iv) If A and $A_1 \subset A$ are both elements of $\mathcal{E}$, then

$$A = \bigcup_{i=1}^{n} A_i,$$

where the sets A_i are pairwise disjoint elements of $\mathcal{E}$, and the first of the sets A_i is the given set A_1.

The following example will make condition (iv) more intuitively accessible: Let $\mathcal{J}$ be a rectangle in the plane whose sides are parallel to the coordinate axes and let $\mathcal{E}$ consist of the empty set $\emptyset$ together with all the rectangles that are contained in $\mathcal{J}$ and whose sides are also parallel to the coordinate axes. Then $\mathcal{E}$ will be a semifield of subsets of $\mathcal{J}$.

Suppose that $\mathcal{E}$ is a semifield of subsets of $\mathcal{J}$, and denote by $\mathcal{F}$ the collection of subsets of $\mathcal{J}$ of the form

$$A = \bigcup_{i=1}^{n} A_i,$$

where n is a positive integer , and the A_i are pairwise disjoint elements of $\mathcal{E}$. Then it is easily shown that $\mathcal{F}$ is a field, i.e., that $\mathcal{F}$ is closed under union, intersection and complementation. In order to show that $\mathcal{F}$ is closed under intersection, for example, note that if $A, B \in \mathcal{F}$, then $A = \bigcup_{i=1}^{n} A_i$ for some pairwise disjoint elements $A_1, \ldots, A_n$ of $\mathcal{E}$ and $B = \bigcup_{j=1}^{m} B_j$ for some pairwise disjoint elements $B_1, \ldots, B_m$ of $\mathcal{E}$. So

$$A \cap B = \left(\bigcup_{i=1}^{n} A_i\right) \cap \left(\bigcup_{j=1}^{m} B_j\right) = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} (A_i \cap B_j).$$

But the $A_i \cap B_j$ are certainly pairwise disjoint and are all in $\mathcal{E}$, by clause (iii) of the definition of a semifield. Hence $A \cap B$ is an element of $\mathcal{F}$.

On the other hand, it is evident that any field of subsets of $\mathcal{J}$ that contains $\mathcal{E}$ must contain $\mathcal{F}$; hence $\mathcal{F}$ must be the smallest field of subsets of $\mathcal{J}$ containing $\mathcal{E}$, which is sometimes called the field of subsets of $\mathcal{J}$ generated by $\mathcal{E}$. We are led, therefore, to the following theorem.

Theorem. If $\mathcal{E}$ is a semifield of subsets of $\mathcal{S}$, then the field of subsets of $\mathcal{S}$ generated by $\mathcal{E}$ consists of those subsets of $\mathcal{S}$ that admit of a disjoint partition into elements of $\mathcal{E}$.

We are now prepared to attack the problem of extending a measure on $\mathcal{E}$.

Definition. A function μ: $\to [0,\infty]$ on a semifield $\mathcal{E}$ of subsets of a set $\mathcal{S}$ is a measure if whenever

$$A = \bigcup_{i=1}^{n} A_i$$

is a finite partition of A, and A, $A_1, \ldots, A_n \in \mathcal{E}$,

$$\mu(A) = \sum_{i=1}^{n} \mu(A_i).$$

It is easily seen that if μ is a measure, then $\mu(\phi) = 0$. Hence if $\mathcal{E}$ is actually a field and $\mu(\mathcal{S}) = 1$, then the measure μ satisfies the usual rules: $\mu(\phi) = 0$, $\mu(\mathcal{S}) = 1$ and $\mu(S_1 \cup S_2) = \mu(S_1) + \mu(S_2)$ whenever $S_1 \cap S_2 = \phi$.

Theorem. If $\mathcal{E}$ is a semifield of subsets of $\mathcal{S}$, and $\mu: \mathcal{E} \to [0, \infty]$ is a measure, then μ has a unique extension to a measure on the field $\mathcal{F}$ generated by $\mathcal{E}$.

Proof: According to the preceding theorem, any element $A \in \tilde{\mathcal{F}}$ admits of a finite partition $A = \bigcup_i A_i$ into elements of $\mathcal{E}$. Define a function $\nu: \tilde{\mathcal{F}} \to [0, \infty]$ by

$$\nu(A) = \sum_i \mu(A_i).$$

In order to see that the value $\nu(A)$ is independent of the partition, notice that if $A = \bigcup_j B_j$ is another partition of A into elements of $\mathcal{E}$, then since $A_i = \bigcup_j (A_i \cap B_j)$ and $B_j = \bigcup_i (A_i \cap B_j)$ are partitions of the elements A_i and B_j into pairwise disjoint elements of $\mathcal{E}$,

$$\sum_i \mu(A_i) = \sum_i \mu\left(\bigcup_j (A_i \cap B_j)\right) = \sum_i \sum_j \mu(A_i \cap B_j)$$

$$= \sum_j \mu\left(\bigcup_i (A_i \cap B_j)\right) = \sum_j \mu(B_j).$$

The additivity of ν for elements of $\mathcal{F}$ is evident, so ν is indeed a measure on $\mathcal{F}$. To see that ν is the unique measure on $\mathcal{F}$ that extends μ, notice that if ν' were another measure on $\mathcal{F}$ that agreed with μ on $\mathcal{E}$, then ν' would have to satisfy

$$\nu'(A) = \sum_i \nu'(A_i) = \sum_i \nu(A_i) = \nu(A)$$

for any element A of $\mathcal{F}$ admitting a finite partition into elements A_i of $\mathcal{E}$. ▨

8. The Representation Theorem: General Case

Theorem. Suppose Bel: $\mathcal{A} \to [0, 1]$ is a belief function. Then there exists a measure algebra $(\mathcal{M}, \mu)$ and an allocation $\rho: \mathcal{A} \to \mathcal{M}$ such that Bel $= \mu \circ \rho$.

The rest of this section is devoted to the proof of this theorem. The corresponding theorem in the finite case was proven by constructing $\mathcal{M}$ as the field of all subsets of the set of non-zero elements of $\mathcal{A}$. In the present proof, we will have to content ourselves with a smaller field of subsets of that set.

Let $\mathcal{J} = \mathcal{A} - \{\Lambda_{\mathcal{A}}\}$, and for each non-empty finite subset $\mathcal{C}$ of $\mathcal{A}$ set

$$R(\mathcal{C}) = \{A \mid A \in \mathcal{J};\ A \leq C \text{ for some } C \in \mathcal{C}\} \subset \mathcal{J},$$

and set

$$\beta(\mathcal{C}) = \beta(A_1, \ldots, A_n),$$

where $A_1, \ldots, A_n$ are the elements of $\mathcal{C}$ and $\beta(A_1, \ldots, A_n)$ is defined as in section 5. If $\mathcal{C} = \phi$, set $R(\mathcal{C}) = \phi$ and $\beta(\mathcal{C}) = 0$. Set

$$\mathcal{R} = \{R(\mathcal{C}) \mid \mathcal{C} \subset \mathcal{A};\ \mathcal{C} \text{ finite}\}.$$

There is a natural way to map $\mathcal{A}$ into $\mathcal{R}$; one simply maps A to $R(\{A\})$. The strategy of this proof will be to develop this mapping into an allocation by extending $\mathcal{R}$ to a field of subsets of $\mathcal{J}$ and using the quantities $\beta(\mathcal{C})$ to define a measure on that field.

Throughout this proof, the letters $\mathcal{C}$, $\mathcal{D}$, $\mathcal{G}$ and $\mathcal{H}$ will always denote finite subsets of $\mathcal{A}$, and the letters A, C and D will always denote elements of $\mathcal{A}$. $\mathcal{C}_A$ will denote the finite subset of $\mathcal{A}$ given by

$$\mathcal{C}_A = \{A \wedge C \mid C \in \mathcal{C}\},$$

and $\mathcal{C} \boxtimes \mathcal{D}$ will denote the finite subset of $\mathcal{A}$ given by

$$\mathcal{C} \boxtimes \mathcal{D} = \{C \wedge D \mid C \in \mathcal{C}, D \in \mathcal{D}\}.$$

Evidently, $\mathcal{C} \boxtimes \mathcal{D} = \mathcal{D} \boxtimes \mathcal{C}$, and $\mathcal{C} \boxtimes \{A\} = \mathcal{C}_A$. Notice also that a distributive law holds for $\boxtimes$ and $\cup$:

$$(\mathcal{C} \cup \mathcal{D}) \boxtimes \mathcal{G} = (\mathcal{C} \boxtimes \mathcal{G}) \cup (\mathcal{D} \boxtimes \mathcal{G}).$$

Let us say that $\mathcal{C}$ majorizes $\mathcal{D}$ if for each non-zero $D \in \mathcal{D}$ there exists an element $C \in \mathcal{C}$ such that $D \leq C$. I will use the notation "$\mathcal{D} \alpha \mathcal{C}$" to indicate that $\mathcal{C}$ majorizes $\mathcal{D}$. The following facts follow from section 5:

(1) If $\mathcal{D} \alpha \mathcal{C}$, then $0 \leq \beta(\mathcal{D}) \leq \beta(\mathcal{C}) \leq 1$.

(2) $\beta(\mathcal{C} \cup \{A\}) = \beta(\mathcal{C}) + \beta(\{A\}) - \beta(\mathcal{C}_A)$.

(3) If $\mathcal{D} \alpha \mathcal{C}$ and $\mathcal{C}_A \alpha \mathcal{D}$ for each $A \in \mathcal{G}$, then

$$\beta(\mathcal{C} \cup \mathcal{G}) - \beta(\mathcal{D} \cup \mathcal{G}) = \beta(\mathcal{C}) - \beta(\mathcal{D}).$$

Now it is obvious that $R(\mathcal{D}) \subset R(\mathcal{C})$ if and only if $\mathcal{D} \alpha \mathcal{C}$. This implies in particular that if $R(\mathcal{D}) = R(\mathcal{C})$, then $\beta(\mathcal{D}) = \beta(\mathcal{C})$. So we can define a mapping

$$b_o : \mathcal{R} \longrightarrow [0, 1]$$

by setting

$$b_o(R(\mathcal{C})) = \beta(\mathcal{C}).$$

Now the collection $\mathcal{R}$ of subsets of $\mathcal{J}$ is closed under the operations of union and intersection. As a matter of fact,

$$R(\mathcal{C}) \cup R(\mathcal{D}) = R(\mathcal{C} \cup \mathcal{D})$$

and

$$R(\mathcal{C}) \cap R(\mathcal{D}) = R(\mathcal{C} \boxtimes \mathcal{D}).$$

Notice that these relations imply in particular that

$$R(\mathcal{C}) - R(\mathcal{D}) = R(\mathcal{C} \cup \mathcal{D}) - R(\mathcal{D}) = R(\mathcal{C}) - R(\mathcal{C} \boxtimes \mathcal{D}) \text{ for all}$$

finite subsets $\mathcal{C}, \mathcal{D}$ of $\mathcal{Q}$.

Our first step in enlarging $\mathcal{R}$ will be to include all differences. Set:

$$\mathcal{E} = \{R_1 - R_2 | R_1, R_2 \in \mathcal{R}\} = \{R(\mathcal{C}) - R(\mathcal{D}) | \ \mathcal{C}, \mathcal{D} \text{ are finite subsets of } \mathcal{Q}\}.$$

Notice that if $E = R(\mathcal{C}) - R(\mathcal{D})$ is in $\mathcal{E}$, then E can also be expressed in the form $E = R(\mathcal{C} \cup \mathcal{D}) - R(\mathcal{D})$. Hence every element of $\mathcal{E}$ is of the form $R_1 - R_2$ where $R_2 \subset R_1$, i.e., of the form $R(\mathcal{C}) - R(\mathcal{D})$, where $\mathcal{D} \alpha \mathcal{C}$.

<u>Lemma 1.</u> $\mathcal{E}$ is a semifield of subsets of $\mathcal{J}$.

Proof: (i) $\phi = R(\phi) - R(\phi)$ is in $\mathcal{E}$.

(ii) $\mathcal{J} = R(\{\nabla\}) - R(\phi)$ is in $\mathcal{E}$.

(iii) Suppose $E_1 = R(\mathcal{C}_1) - R(\mathcal{A}_1)$ and $E_2 = R(\mathcal{C}_2) - R(\mathcal{A}_2)$ are in $\mathcal{E}$.

Then

$$E_1 \cap E_2 = (R(\mathcal{C}_1) \cap \overline{R(\mathcal{A}_1)}) \cap (R(\mathcal{C}_2) \cap \overline{R(\mathcal{A}_2)})$$

$$= (R(\mathcal{C}_1) \cap R(\mathcal{C}_2)) \cap \overline{R(\mathcal{A}_1) \cup R(\mathcal{A}_2)}$$

$$= R(\mathcal{C}_1 \boxtimes \mathcal{C}_2) \cap \overline{R(\mathcal{A}_1 \cup \mathcal{A}_2)}$$

$$= R(\mathcal{C}_1 \boxtimes \mathcal{C}_2) - R(\mathcal{A}_1 \cup \mathcal{A}_2)$$

is in $\mathcal{E}$.

(iv) Suppose $E_1 = R(\mathcal{C}_1) - R(\mathcal{A}_1)$ and $E_2 = R(\mathcal{C}_2) - R(\mathcal{A}_2)$ are in $\mathcal{E}$, and $E_1 \subset E_2$. Then one may assume that $R(\mathcal{A}_1) \subset R(\mathcal{C}_1)$, so that

$$\overline{E_1} = \overline{R(\mathcal{C}_1) \cap \overline{R(\mathcal{A}_1)}} = \overline{R(\mathcal{C}_1)} \cup R(\mathcal{A}_1)$$

will be a disjoint partition of $\overline{E}_1$. Then

$$E_2 - E_1 = E_2 \cap \overline{E}_1 = (E_2 \cap \overline{R(\mathcal{C}_1)}) \cup (E_2 \cap R(\mathcal{A}_1))$$

will also be a disjoint partition. But

$$E_2 \cap \overline{R(\mathcal{C}_1)} = R(\mathcal{C}_2) \cap \overline{R(\mathcal{A}_2)} \cap \overline{R(\mathcal{C}_1)}$$

$$= R(\mathcal{C}_2) \cap \overline{R(\mathcal{A}_2 \cup \mathcal{C}_1)}$$

is in $\mathcal{E}$, and

$$E_2 \cap R(\mathcal{A}_1) = R(\mathcal{C}_2) \cap \overline{R(\mathcal{A}_2)} \cap R(\mathcal{A}_1)$$

$$= R(\mathcal{C}_2 \boxtimes \mathcal{A}_1) \cap \overline{R(\mathcal{A}_2)}$$

is in $\mathcal{E}$, so we have expressed $E_2 - E_1$ as a disjoint partition of elements of $\mathcal{E}$, as required. ▨

Lemma 2. If $\mathcal{A} \alpha \mathcal{C}$ and $(R(\mathcal{C}) - R(\mathcal{A})) \cap R(\mathcal{G}) = \phi$, then

$$\text{(i)} \quad R(\mathcal{C} \cup \mathcal{G}) - R(\mathcal{A} \cup \mathcal{G}) = R(\mathcal{C}) - R(\mathcal{A})$$

$$\text{and (ii)} \quad \beta(\mathcal{C} \cup \mathcal{G}) - \beta(\mathcal{A} \cup \mathcal{G}) = \beta(\mathcal{C}) - \beta(\mathcal{A}).$$

Proof. From the hypothesis it immediately follows that

$$(R(\mathcal{C}) \cup R(\mathcal{G})) - (R(\mathcal{A}) \cup R(\mathcal{G})) = R(\mathcal{C}) - R(\mathcal{A}),$$

whence (i). Consider now any elements $C \in \mathcal{C}$ and $A \in \mathcal{G}$. If $C \wedge A \neq \Lambda$, then $C \wedge A$ is in both $R(\mathcal{C})$ and $R(\mathcal{G})$, and hence must be in $R(\mathcal{A})$; hence there must exist an element $D \in \mathcal{A}$ such that $C \wedge A \leq D$. If $C \wedge A = \Lambda$, on the other hand, then $C \wedge A \leq D$ for any $D \in \mathcal{A}$. In any case, $\mathcal{C}_A \alpha \mathcal{A}$ for all $A \in \mathcal{G}$, and (ii) follows from (3) above. ▨

Lemma 3. If $\mathcal{A} \alpha \mathcal{C}$, $\mathcal{H} \alpha \mathcal{G}$, and

$$R(\mathcal{C}) - R(\mathcal{A}) = R(\mathcal{G}) - R(\mathcal{H}),$$

then $$\beta(\mathcal{C}) - \beta(\mathcal{A}) = \beta(\mathcal{G}) - \beta(\mathcal{H}).$$

Proof: Since $R(\mathcal{H}) \cap (R(\mathcal{G}) - R(\mathcal{H})) = \phi$, the hypothesis of the lemma implies that $R(\mathcal{H}) \cap (R(\mathcal{C}) - R(\mathcal{A})) = \phi$. By Lemma 2,

$$\text{(i)} \quad R(\mathcal{C}) - R(\mathcal{A}) = R(\mathcal{C} \cup \mathcal{H}) - R(\mathcal{A} \cup \mathcal{H})$$

$$\text{and} \quad \text{(ii)} \quad \beta(\mathcal{C}) - \beta(\mathcal{A}) = \beta(\mathcal{C} \cup \mathcal{H}) - \beta(\mathcal{A} \cup \mathcal{H}).$$

Symmetrically,

$$\text{(iii)} \quad R(\mathcal{G}) - R(\mathcal{H}) = R(\mathcal{G} \cup \mathcal{A}) - R(\mathcal{H} \cup \mathcal{A})$$

$$\text{and} \quad \text{(iv)} \quad \beta(\mathcal{G}) - \beta(\mathcal{H}) = \beta(\mathcal{G} \cup \mathcal{A}) - \beta(\mathcal{H} \cup \mathcal{A}).$$

It follows from (i), (iii) and the hypothesis of the lemma that

$$R(\mathcal{G} \cup \mathcal{A}) - R(\mathcal{H} \cup \mathcal{A}) = R(\mathcal{C} \cup \mathcal{H}) - R(\mathcal{A} \cup \mathcal{H}),$$

whence $R(\mathcal{G} \cup \mathcal{A}) = R(\mathcal{C} \cup \mathcal{H})$. Hence $\beta(\mathcal{G} \cup \mathcal{A}) = \beta(\mathcal{C} \cup \mathcal{H})$. From (ii) and (iv) it then follows that

$$\beta(\mathcal{C}) - \beta(\mathcal{D}) = \beta(\mathcal{G}) - \beta(\mathcal{H}).$$

Lemma 4. If $\mathcal{D}\ \alpha\, \mathcal{C}$ and $(R(\mathcal{C}) - R(\mathcal{D})) \subset R(\mathcal{G})$, then

(i) $R(\mathcal{C} \boxtimes \mathcal{G}) - R(\mathcal{D} \boxtimes \mathcal{G}) = R(\mathcal{C}) - R(\mathcal{D})$

and (ii) $\beta(\mathcal{C} \boxtimes \mathcal{G}) - \beta(\mathcal{D} \boxtimes \mathcal{G}) = \beta(\mathcal{C}) - \beta(\mathcal{D})$.

Proof: From the hypothesis it immediately follows that

$$(R(\mathcal{C}) \cap R(\mathcal{G})) - (R(\mathcal{C}) \cap R(\mathcal{D})) = R(\mathcal{C}) - R(\mathcal{D}),$$

whence (i). The second relation then follows by lemma 3. ▨

Every element of $\mathcal{E}$ can be written in the form $R(\mathcal{C}) - R(\mathcal{D})$, with $\mathcal{D}\,\alpha\,\mathcal{C}$; and according to lemma 3, $\beta(\mathcal{C}) - \beta(\mathcal{D})$ does not depend on the choice of $\mathcal{C}$ and $\mathcal{D}$. Hence a function $b: \mathcal{E} \to [0, 1]$ may be defined by setting $b(E) = \beta(\mathcal{C}) - \beta(\mathcal{D})$ when $E = R(\mathcal{C}) - R(\mathcal{D}$ and $\mathcal{D}\,\alpha\,\mathcal{C}$. The function b is obviously an extension of the function $b_o: \mathcal{R} \to [0, 1]$.

Now let $\mathcal{M}$ be the field of subsets of $\mathcal{T}'$ generated by $\mathcal{E}$, and define a mapping $\rho: \mathcal{A} \to \mathcal{M}$ by $\rho(A) = R(\{A\})$. It is easily verified that

(i) $\rho(V) = R(\{V\}) = \mathcal{T}'$.

(ii) $\rho(\Lambda) = R(\{\Lambda\}) = \phi$.

(iii) $\rho(A_1 \cap A_2) = R(\{A_1 \cap A_2\}) = R(\{A_1\} \boxtimes \{A_2\} = R(\{A_1\}) \cap R(\{A_2\})$
$= \rho(A_1) \cap \rho(A_2)$.

Hence ρ is a non-singular allocation. Furthermore, for each $A \in \mathcal{A}$, $Bel(A) = \beta(\{A\}) = b(R(\{A\})) = b(\rho(A))$. Hence if b could be extended to a measure μ on $\mathcal{M}$, then Bel would be the belief function induced by the allocation ρ into the probability algebra $(\mathcal{M}, \mu)$, and the proof would be complete. But we learned in section 5 that b can be extended to a probability function μ on $\mathcal{M}$ provided that b is a measure on $\mathcal{E}$. Hence our only remaining task is to show that b is a measure.

In order to show that b is a measure, one must show that if $E = E_1 \cup \ldots \cup E_n$ is a disjoint partition of E and if E, $E_1, \ldots, E_n \in \mathcal{E}$, then $b(E) = \sum_{i=1}^{n} b(E_i)$. In order to carry out such a demonstration, let us fix E and the E_i and express them in the form

$$E = R(\mathcal{C}) - R(\mathcal{D})$$

and

$$E_i = R(\mathcal{C}_i) - R(\mathcal{D}_i)$$

for i = 1, ..., n. We may assume that $\mathcal{D} \alpha \mathcal{C}$ and $\mathcal{D}_i \alpha \mathcal{C}_i$ for i = 1, ..., n. We may also assume that $\mathcal{C}_i \alpha \mathcal{C}$ for i = 1, ..., n, for if this did not hold then the $\mathcal{C}_i$ and the $\mathcal{D}_i$ could be replaced by the sets $\mathcal{C}_i \boxtimes \mathcal{C}$ and $\mathcal{D}_i \boxtimes \mathcal{D}$, respectively.

Set

$$\mathcal{W} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_n \cup \mathcal{D}_1 \cup \ldots \cup \mathcal{D}_n \cup \mathcal{C} \cup \mathcal{D},$$

and set

$$\mathcal{V} = \{A_1 \wedge \ldots \wedge A_n \mid n \geq 1 \text{ and } A_1, \ldots, A_n \in \mathcal{W}\}.$$

Then $\mathcal{V}$ is finite, $\mathcal{W} \subset \mathcal{V}$, $\mathcal{V} \alpha \mathcal{C}$, and $\mathcal{V}$ is closed under conjunctions, i.e., if A and A' are in $\mathcal{V}$, then $A \wedge A'$ is in $\mathcal{V}$. The partial ordering that $\mathcal{V}$ inherits from $\mathcal{Q}$ (see Chapter 3, section 1) can be extended to a total ordering on $\mathcal{V}$, i.e., the elements of $\mathcal{V}$ can be indexed $V_1, \ldots, V_r$ so that if $V_s \leq V_t$, then $s \leq t$. Suppose this is done, and set $\mathcal{V}_s = \{V_t \mid t \leq s\}$ for s = 1, ..., r. Set $V_o = \phi$.

For each s, s = 1, ..., r, set

$$R_s = R(\mathcal{D} \cup \mathcal{V}_s) - R(\mathcal{D} \cup \mathcal{V}_{s-1})$$

and

$$\beta_s = \beta(\mathcal{D} \cup \mathcal{V}_s) - \beta(\mathcal{D} \cup \mathcal{V}_{s-1}).$$

Notice that $R_s \subset E$ for s = 1, ..., r; for $\mathcal{D} \cup \mathcal{V}_s \alpha \mathcal{C}$ and $\mathcal{D} \alpha \mathcal{D} \cup \mathcal{V}_{s-1}$.

Lemma 5. For each s, s = 1, ..., r, there exists an integer k between 1 and n such that $R_s \subset E_k$.

Proof: Since $R(\mathcal{A} \cup \mathcal{V}_s) = R(\mathcal{A} \cup \mathcal{V}_{s-1}) \cup R(\{V_s\})$,

$$R_s = R(\{V_s\}) - R(\mathcal{A} \cup \mathcal{V}_{s-1}).$$

If $R_s = \phi$, then the conclusion of the lemma follows trivially, so it may be supposed that $R_s \neq \phi$. In this case, V_s must be in R_s and hence in E. Let K be the integer for which $V_s \in E_K$. Then there must exist an element $C \in \mathcal{C}_K$ such that $V_x \leq C$, but V_s cannot satisfy $V_s \leq V$ for any $V \in \mathcal{D}_K$. We must now show that any other element $A \in R_s$ must also be in E_K. But if $A \in R_s$, then A satisfies $A \leq V_s \leq C$ and fails to satisfy $A \leq V_t$ for any other element V_t such that $t < s$. Since $C \in \mathcal{C}_K$, $A \in R(\mathcal{C}_K)$, and it suffices to show that $A \notin R(\mathcal{D}_K)$ -- i.e., that $A \leq D$ does not hold for any $D \in \mathcal{D}_K$.

Let us suppose that $A \leq D$ does hold for a given $D \in \mathcal{D}_K$ and derive a contradiction. Indeed, if $A \leq D$, then $A \leq V_s \wedge D$. But since $V_s \in E_K$, $V_s \leq D$ does not hold, and hence $V_s \wedge D$ must be a proper sub-element of V_s and is therefore equal to V_t for some $t < s$. Since we have $A \leq V_t$ for some t such that $t < s$, this is our contradiction. ▨

It follows from lemma 5 that the set $\{1, \ldots, r\}$ can be partitioned into n disjoint sets $N_1, \ldots, N_n$ such that $R_s \subset E_i$ if $s \in N_i$.

If $s \in N_i$, then $R_s \subset E_i$ and $R(\mathcal{D}_i) \cap R_s = \phi$ and $R_s \subset R(\mathcal{C}_i)$, so successive applications of lemmas 2 and 4 result in

$$R_s = R((\mathcal{A} \cup \mathcal{D}_i \cup \mathcal{V}_s) \bowtie \mathcal{C}_i) - R((\mathcal{A} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \bowtie \mathcal{C}_i)$$

and

$$\beta_s = \beta((\mathcal{A} \cup \mathcal{D}_i \cup \mathcal{V}_s) \bowtie \mathcal{C}_i) - \beta((\mathcal{A} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \bowtie \mathcal{C}_i).$$

If, on the other hand, $s \notin N_i$, then either $R_s = \phi$ or R_s is not contained in E_i. In either case,

$$
\begin{aligned}
\phi &= R_s \cap E_i \\
&= (R(\mathcal{D} \cup \mathcal{V}_s) - R(\mathcal{D} \cup \mathcal{V}_{s-1})) \cap (R(\mathcal{C}_i) - R(\mathcal{D}_i)) \\
&= R((\mathcal{D} \cup \mathcal{V}_s) \boxtimes \mathcal{C}_i) - R(\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \\
&= R((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_s) \boxtimes \mathcal{C}_i) - R((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \boxtimes \mathcal{C}_i).
\end{aligned}
$$

Hence the quantity

$$
\beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_s) \boxtimes \mathcal{C}_i) - \beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \boxtimes \mathcal{C}_i)
$$

is equal to β_s if $s \in N_i$ and zero if $s \notin N_i$. Consequently,

$$
\begin{aligned}
\sum_{s \in N_i} \beta_s &= \sum_{s=1}^{r} (\beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_s) \boxtimes \mathcal{C}_i) - \beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_{s-1}) \boxtimes \mathcal{C}_i)) \\
&= \beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_r) \boxtimes \mathcal{C}_i) - \beta((\mathcal{D} \cup \mathcal{D}_i \cup \mathcal{V}_o) \boxtimes \mathcal{C}_i) \\
&= \beta(\mathcal{C}_i) - \beta(\mathcal{D}_i) = b(E_i).
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
\sum_{s=1}^{r} \beta_s &= \sum_{s=1}^{r} (\beta(\mathcal{D} \cup \mathcal{V}_s) - \beta(\mathcal{D} \cup \mathcal{V}_{s-1})) \\
&= \beta(\mathcal{D} \cup \mathcal{V}_r) - \beta(\mathcal{D}) = \beta(\mathcal{C}) - \beta(\mathcal{D}) = b(E);
\end{aligned}
$$

hence

$$
\sum_{i=1}^{r} b(E_i) = \sum_{i=1}^{r} \sum_{s \in N_i} \beta_s = \sum_{s=1}^{r} \beta_s = b(E),
$$

and b is indeed a measure on $\mathcal{E}$. This completes the proof of the theorem.

9. The Constraint Mapping

Recall that an allocation of probability $\rho: \mathcal{Q} \rightarrow \mathcal{M}$ is said to specify the constraint relation "ct" between $\mathcal{M}$ and $\mathcal{Q}$ whenever " M ct A " is equivalent to $M \leq \rho(A)$. Obviously, ρ and ct are two different ways of conveying exactly the same information, but our attention is concentrated on ρ whenever we attend to a particular proposition $A \varepsilon \mathcal{Q}$ and ask about the probability that is constrained to A. For $\rho(A)$ is the "largest" probability mass constrained to A, in the sense that the probability masses constrained to A are precisely those which are subelements of $\rho(A)$.

But suppose we fix our attention on a particular probability mass $M \varepsilon \mathcal{M}$ and contemplate all the elements of $\mathcal{Q}$ to which M is constrained. Then there may or may not be a "smallest" element $\lambda(M)$ among these. In other words, there may or may not be an element $\lambda(M) \varepsilon \mathcal{Q}$ such that M is constrained to any given element $A \varepsilon \mathcal{Q}$ if and only if $\lambda(M) \leq A$. If there is such an element $\lambda(M) \varepsilon \mathcal{Q}$ for each $M \varepsilon \mathcal{M}$, then I will call the mapping $\lambda: \mathcal{M} \rightarrow \mathcal{Q}: M \rightsquigarrow \lambda(M)$ the constraint mapping for ρ and ct ; for the mapping λ will specify the "tightest" constraint for each probability mass.

The following definition lists the properties of constraint mappings.

Definition. Suppose $\mathcal{Q}$ is a Boolean algebra of propositions and $\mathcal{M}$ is a Boolean algebra of probability masses. Then a mapping $\lambda: \mathcal{M} \rightarrow \mathcal{Q}$ is a constraint mapping if

(i) $\lambda(\Lambda_{\mathcal{M}}) = \Lambda_{\mathcal{Q}}$.

(ii) If $\lambda(M) = \Lambda_{\mathcal{Q}}$, then $M = \Lambda_{\mathcal{M}}$.

(iii) $\lambda(M_1 \vee M_2) = \lambda(M_1) \vee \lambda(M_2)$.

One immediate consequence of rule (iii) in this definition is that a constraint mapping λ is monotone, i.e. $\lambda(M_1) \leq \lambda(M_2)$ whenever $M_1 \leq M_2$.

(See Chapter 3, section 3 below.) This formal definition for constraint mappings is justified by the two following propositions.

<u>Theorem</u>. Suppose ct is a constraint relation between a Boolean algebra of probability masses $\mathcal{M}$ and a Boolean algebra of propositions $\mathcal{A}$. And suppose $\lambda: \mathcal{M} \to \mathcal{A}$ is a mapping such that M ct A if and only if $\lambda(M) \leq A$. Then λ is a constraint mapping.

<u>Proof</u>: (i) By rule (2c) for constraint relations, $\Lambda_{\mathcal{M}}$ ct $\Lambda_{\mathcal{A}}$. Hence we must have $\lambda(\Lambda_{\mathcal{M}}) \leq \Lambda_{\mathcal{A}}$, or $\lambda(\Lambda_{\mathcal{M}}) = \Lambda_{\mathcal{A}}$.

(ii) If $\lambda(M) = \perp_{\mathcal{A}}$, the M ct $\perp_{\mathcal{A}}$. Hence, by rule (3) for constraint relations, $M = \perp_{\mathcal{M}}$.

(iii) By hypothesis, M_1 and M_2 are both constrained to a proposition A if and only if $\lambda(M_1) \vee \lambda(M_2) \leq A$. But from rules (2a) and (2b) for constraint relations, M_1 and M_2 are both constrained to A if and only if $M_1 \vee M_2$ is constrained to A. Hence $M_1 \vee M_2$ is constrained to a proposition A if and only if $\lambda(M_1) \vee \lambda(M_2) \leq A$. Hence $\lambda(M_1 \vee M_2) = \lambda(M_1) \vee \lambda(M_2)$. ▨

<u>Theorem</u>. Suppose $\lambda: \mathcal{M} \to \mathcal{A}$ is a constraint mapping. Then the binary relation "ct" between $\mathcal{M}$ and $\mathcal{A}$ defined by "M ct A if and only if $\lambda(M) \leq A$" is a constraint relation. (I will call this the constraint relation given by λ.)

<u>Proof</u>: It is necessary to establish conditions (1), (2) and (3) in the definition of a constraint relation. Condition (1) is immediate; and the others are implied by the three conditions in the definition of a constraint mapping: (i) implies (2c), (ii) implies (3), (iii) implies (2b), and the monotonicity of λ implies (2a). ▨

It should be reiterated that constraint mappings do not always exist, even when an allocation of probability does. In other words, if a constraint relation ct between $\mathcal{M}$ and $\mathcal{A}$ is given directly or by means of an allocation, $\rho: \mathcal{A} \to \mathcal{M}$, then there does not necessarily exist a constraint mapping $\lambda: \mathcal{M} \to \mathcal{A}$ which gives ct. If such a constraint mapping λ does exist, though, it is necessarily unique.

Theorem. Suppose $\mathcal{A}$ is a finite Boolean algebra of propositions, $\mathcal{M}$ is a Boolean algebra of probability masses, and ct is a constraint relation between $\mathcal{M}$ and $\mathcal{A}$. Then a constraint mapping λ exists for ct.

Proof: We can define λ as follows. For each $M \in \mathcal{M}$, let $A_1, \ldots, A_n$ be all the elements of $\mathcal{A}$ to which M is constrained -- by rule (1c) for constraint relations there is at least one of these, and since $\mathcal{A}$ is finite there can only be a finite number of them. Let $\lambda(M)$ equal to $A_1 \wedge \ldots \wedge A_n$. It then follows from rule (1b) for constraint relations that M ct $\lambda(M)$; hence for any $A \in \mathcal{A}$, M ct A if and only if $\lambda(M) \leq A$. It follows from the first theorem in this section that λ is a constraint mapping. ▨

In the preceding section we began with an arbitrary belief function on an arbitrary Boolean algebra of propositions $\mathcal{A}$ and constructed an allocation $\rho: \mathcal{A} \to \mathcal{M}$ that gave that belief function. It is natural to ask whether a constraint mapping $\lambda: \mathcal{M} \to \mathcal{A}$ exists forthe allocation ρ so constructed.

The answer is that a constraint mapping does exist. Indeed, if $M \in \mathcal{M}$, then M is the union of a finite number of disjoint subsets of $\mathcal{J}$ of the form $R(\mathcal{C}_i) - R(\mathcal{L}_i)$ with $\mathcal{L}_i \propto \mathcal{C}_i$. Suppose, indeed, the

$M = \bigcup_{i=1}^{n} (R(\mathcal{C}_i) - R(\mathcal{D}_i))$, where $\mathcal{D}_i \propto \mathcal{C}_i$ and the $R(\mathcal{C}_i) - R(\mathcal{D}_i)$ are disjoint. For each i, i = 1, ..., n, set $\mathcal{C}'_i$ equal to the subset of $\mathcal{C}_i$ consisting of elements not majorized by $\mathcal{D}_i$; i.e., set

$$\mathcal{C}'_i = \mathcal{C}_i - \{C | C \in \mathcal{C}_i \text{ and } C \leq D \text{ for some } D \in \mathcal{D}_i\}.$$

Then

$$R(\mathcal{C}_i) - R(\mathcal{D}_i) = R(\mathcal{C}'_i) - R(\mathcal{D}_i).$$

Set $\mathcal{C} = \bigcup_{i=1}^{n} \mathcal{C}'_i$. Then $\mathcal{C}$ is a finite subset of $\mathcal{A}$, and $\mathcal{C} \subset M$. Set $\lambda(M)$ equal to the disjunction of all the elements of $\mathcal{C}$. In other words, index the elements of $\mathcal{C}$, say $C_1, \ldots, C_k$, and set $\lambda(M) = C_1 \vee \ldots \vee C_K$. If $\mathcal{C} = \phi$ set $\lambda(M) = \Lambda_{\mathcal{A}}$. Then $\{\lambda(M)\}$ majorizes $\mathcal{C}$, and

$$\rho(\lambda(M)) = R(\{C_1 \vee \ldots \vee C_k\}) \supset R(\mathcal{C}) = R(\mathcal{C}_1) \cup \ldots \cup R(\mathcal{C}_n) \supset M.$$

Hence M ct $\lambda(M)$, and M ct A for all A such that $\lambda(M) \leq A$. On the other hand, if $A \in \mathcal{A}$ and M ct A, then $\mathcal{C} \subset M \subset \rho(A) = R(\{A\})$. This implies that $\{A\}$ majorizes $\mathcal{C}$, whence $\lambda(M) \leq A$. Hence an element A of $\mathcal{A}$ satisfies M ct A if and only if $\lambda(M) \leq A$. Thus the mapping $\lambda: \mathcal{M} \rightarrow \mathcal{A}: M \rightsquigarrow \lambda(M)$ is indeed a constraint mapping corresponding to the constraint relation between $\mathcal{M}$ and $\mathcal{A}$.

10. Toward a Better Representation of our Probability

We have now arrived at the conclusion that any belief function on a Boolean algebra $\mathcal{A}$ can be represented by an allocation $\rho: \mathcal{A} \rightarrow \mathcal{M}$ that maps $\mathcal{A}$ into a "measure algebra" $\mathcal{M}$. But as I remarked in section 1, our formal definition of a measure algebra falls somewhat short of imposing all the properties that we might want our idealized "probability" to have. The following three properties are the most important of the additional properties that we might want to require of $(\mathcal{M}, \mu)$:

(i) Positivity: If $M \in \mathcal{M}$ and $M \neq \Lambda_{\mathcal{M}}$, then M ought to have measure: $\mu(M) > 0$.

(ii) Completeness: If $\{M_\gamma\}_{\gamma \in \Gamma}$ is any collection of elements of $\mathcal{M}$, then there ought to be an element of $\mathcal{M}$ representing their union and another representing their intersection.

(iii) Complete Additivity: Suppose $\{M_\gamma\}_{\gamma \in \Gamma}$ is a disjoint collection of elements of $\mathcal{M}$. In other words, suppose $M_\gamma \wedge M_{\gamma'} = \Lambda_{\mathcal{M}}$ for all distincts pairs, γ, γ' in Γ. Then the measure of their union ought to be equal to $\sum_\gamma \mu(M_\gamma)$.

These three properties may seem too strong for us to expect that our measure algebra $\mathcal{M}$ should have them. But in fact we can always arrange that $\mathcal{M}$ should have them.

Unfortunately, though, the demonstration of this fact can hardly be carried out without a more thorough knowledge of the mathematics of Boolean algebras. Hence we must turn to an examination of the theory of lattices and Boolean algebras, an examination that is already long overdue.

CHAPTER 3. THE THEORY OF BOOLEAN ALGEBRAS

This chapter is intended as a brief and sketchy introduction to the abstract theory of Boolean algebras. Almost all its vocabulary, assertions and theorems are standard in that theory. For a more thorough study of the subject, the reader may wish to consult Garrett Birkhoff's Lattice Theory, Roman Sikorski's Boolean Algebras, or Paul Halmos' Lectures on Boolean Algebras.

1. Partially Ordered Sets

A binary relation between two sets $\mathcal{A}$ and $\mathcal{B}$ is a subset r of the Cartesian product $\mathcal{A} \times \mathcal{B}$. If $(A, B) \in r$, then one says that the binary relation r holds between A and B, and one writes "A r B." A binary relation "$\leq$" between a set $\mathcal{A}$ and itself is called a partial ordering if

(1) $A \leq A$ for all $A \in \mathcal{A}$.

(2) If $A \leq B$ and $B \leq C$, then $A \leq C$.

(3) If $A \leq B$ and $B \leq A$, then $A = B$.

If a non-empty set has associated with it a partial ordering, then it is called a partially ordered set. If A and B are in a partially ordered set and $A \leq B$, then A is said to minorize B or to be a subelement of B, while B is said to majorize A. If $A \leq B$, and $A \neq B$, then one writes $A < B$ and says that A is a proper subelement of B.

Examples of partially ordered sets abound in mathematics. For example, any set $\mathcal{A}$ of sets becomes a partially ordered set if it is endowed with the partial ordering

$$\leq \; = \{(A, B) \mid A, B \in \mathcal{A} ; A \subset B\},$$

i.e., if it is partially ordered by set inclusion. Other examples are provided by the usual "less than or equal" orderings of numbers.

A partial ordering $\leq$ on a set $\mathcal{A}$ is a <u>total ordering</u> if for every pair $A, B \in \mathcal{A}$, either $A \leq B$ or $B \leq A$.

<u>Theorem</u>. A partial ordering on a finite set can always be extended to a total ordering. More explicitly, if $\leq_o$ is a partial ordering on a finite set $\mathcal{A}$, then there is a total ordering $\leq$ on $\mathcal{A}$ such that $\leq_o \subset \leq$.

<u>Proof</u>: Suppose $\leq_o$ is not a total ordering on $\mathcal{A}$. Then let A, B be elements of $\mathcal{A}$ such that neither $A \leq B$ nor $B \leq A$. Then set

$$\leq_1 \; = \; \leq_o \cup \{(C, D) \mid C \in \mathcal{A} ; D \in \mathcal{A} ; C \leq_o A ; B \leq_o D\}.$$

It is easily verified that $\leq_1$ is a partial ordering on $\mathcal{A}$ and that $A \leq_1 B$.

Hence a partial ordering can always be extended to make a given "non-comparable" pair comparable. Since $\mathcal{A}$ is finite, one can have only a finite number, say n, of non-comparable pairs; hence the theorem follows by induction. ▨

If $\mathcal{C}$ is a subset of a partially ordered set $\mathcal{A}$, then there can be at most one element $C \in \mathcal{C}$ such that for all $B \in \mathcal{C}$, $C \leq B$. For if there were two such elements C_1 and C_2 in $\mathcal{C}$, then they would satisfy $C_1 \leq C_2$ and $C_2 \leq C_1$ and hence, by (3), $C_1 = C_2$. If such an element does exist it is, quite naturally, called the <u>least</u> element of $\mathcal{C}$. Similarly, $\mathcal{C}$ may or may not have a <u>greatest</u> element -- i.e., an element $C \in \mathcal{C}$ such that for all $B \in \mathcal{C}$, $B \leq C$; but if there is such an element, it is unique. If the partially ordered set $\mathcal{A}$ itself has a least element, that element is called the zero of $\mathcal{A}$, and denoted $\perp_{\mathcal{A}}$ or $\perp$; if it has a greatest element, that element is called the unit of $\mathcal{A}$ and denoted $\top_{\mathcal{A}}$ or $\top$.

If $\mathcal{C}$ is a subset of a partially ordered set $\mathcal{A}$, then an element $A \in \mathcal{A}$ is called a lower bound of $\mathcal{C}$ if $A \leq C$ for all $C \in \mathcal{C}$, and an element $A \in \mathcal{A}$ is called an upper bound of $\mathcal{C}$ if $C \leq A$ for all $C \in \mathcal{C}$. It is possible for a given proper subset $\mathcal{C}$ of $\mathcal{A}$ to have many lower and upper bounds in $\mathcal{A}$, but $\mathcal{A}$ itself can have at most one lower bound and one upper bound. For the lower bound of $\mathcal{A}$, if it exists, is its zero; and the upper bound, if it exists, is its unit. The zero and unit of $\mathcal{A}$ are sometimes called the universal bounds of $\mathcal{A}$.

Let $\mathcal{C}$ be a given subset of a partially ordered set $\mathcal{A}$, and let $\mathcal{L} \subset \mathcal{A}$ be the collection of all the lower bounds of $\mathcal{C}$. The set $\mathcal{L}$ may or may not be empty, and if it is not empty, then it may or may not have a greatest element. If $\mathcal{L}$ is non-empty, and does have a greatest element, then that element is called, quite naturally, the greatest lower bound of $\mathcal{C}$; it is also called the meet of the elements of $\mathcal{C}$. Similarly, if the collection $\mathcal{U}$ of all upper bounds of $\mathcal{C}$ is non-empty and has a least element, then that element is called the least upper bound of $\mathcal{C}$, or the join of the elements of $\mathcal{C}$.

The notions of meet and join are of central importance in lattice theory, and it may be worthwhile to repeat their definitions in a less verbal way, replacing the set $\mathcal{C}$ with an indexed collection $\{A_\gamma\}_{\gamma \in \Gamma}$ of elements of $\mathcal{A}$: The meet of a collection $\{A_\gamma\}_{\gamma \in \Gamma}$ is the element $A \in \mathcal{A}$, unique if it exists, such that $A \leq A_\gamma$ for all $\gamma \in \Gamma$ and $B \leq A$ if $B \in \mathcal{A}$ is any other element satisfying $B \leq A_\gamma$ for all $\gamma \in \Gamma$. The join of a collection $\{A_\gamma\}_{\gamma \in \Gamma}$ is the element $A \in \mathcal{A}$, unique if it exists, such that $A_\gamma \leq A$ for all $\gamma \in \Gamma$ and $A \leq B$ if $B \in \mathcal{A}$ is any other element satisfying $A_\gamma \leq B$ for all $\gamma \in \Gamma$.

It should be borne in mind that the notions of meet and join are relative to a fixed partially ordered set $\mathcal{A}$. For it is possible that a subset $\mathcal{C}$ of a partially ordered set $\mathcal{A}$ might also be a subset of a different partially ordered set $\mathcal{B}$; in such a case, $\mathcal{C}$ might have, say, one meet in $\mathcal{A}$ and a different one in $\mathcal{B}$ -- or perhaps a meet in $\mathcal{A}$ and no meet at all in $\mathcal{B}$.

The symbol "$\wedge$" usually is used to denote a meet: the meet of $\mathcal{C} \subset \mathcal{A}$ is denoted by $\wedge \mathcal{C}$, the meet of a collection $\{A_\gamma\}_{\gamma \in \Gamma}$ of elements of $\mathcal{A}$ is denoted by $\underset{\gamma}{\wedge} A_\gamma$ or $\wedge A_\gamma$, and the meet of a pair of elements A and B of $\mathcal{A}$ is denoted by $A \wedge B$. The symbol "$\vee$" is used analogously for joins; one writes $\vee \mathcal{C}$, $\underset{\gamma}{\vee} A_\gamma$ or $\vee A_\gamma$, and $A \vee B$. The similarity between this notation and the notation for intersection and union in the theory of sets is justified by the fact that if $\mathcal{A}$ is a collection of subsets of a given set and $\mathcal{A}$ is closed under the operations of union and intersection, then $\mathcal{A}$ is partially ordered by set inclusion and every collection $\{A_\gamma\}_{\gamma \in \Gamma}$ of elements of has a meet and a join, which are given by the intersection and union respectively.

A partially ordered set $\mathcal{A}$ is called a meet-semilattice if every pair of elements in $\mathcal{A}$ have a meet in $\mathcal{A}$. Similarly, it is called a join-semilattice if every pair of elements has a join, and simply a lattice if every pair of elements has both a meet and a join.

It is easily deduced that meets and joins exist for all finite collections of elements in a lattice. They need not exist, however, for infinite collections. A lattice for which they all do exist is said to be complete. A finite lattice is necessarily complete. Actually, the existence of meets for all collections of elements in a lattice implies the existence of joins for all collections and hence implies completeness; similarly, the existence of joins for all collections implies completeness.

If meets and joins exist for all countable collections of elements in a lattice, then the lattice is said to be σ-complete. Of course, a complete lattice is σ-complete. The existence either of meets for all countable collections or of joins for all countable collections is sufficient to assure σ-completeness.

Notice that a complete lattice necessarily has universal bounds, for the meet of all the elements of the lattice will be the zero, and the join of all the elements of the lattice will be the unit.

If a partially ordered set has only one element, then that element will be both the zero and the unit, but if the set has more than one element, then the zero and unit must be distinct if they both exist. It is easily seen that if $\curlywedge$ is the zero of a partially ordered set $\mathcal{Q}$ and $A \in \mathcal{Q}$, then $A \wedge \curlywedge = \curlywedge$ and $A \vee \curlywedge = A$. Similarly if $\curlyvee$ if the unit of $\mathcal{Q}$ and $A \in \mathcal{Q}$, then $A \wedge \curlyvee = A$ and $A \vee \curlyvee = \curlyvee$.

If A, B and C are elements of a lattice and $B \leq C$, then $B \vee A \leq C \vee A$ and $B \wedge A \leq C \wedge A$.

A lattice is distributive if all triplets of elements A, B, C in the lattice satisfy

$$(1) \quad A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

and

$$(2) \quad A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$

Actually, either of rules (1) and (2) implies the other. They also imply various infinite distributive laws. Among them:

$$A \wedge (\bigvee_{\gamma} A_{\gamma}) = \bigvee_{\gamma} (A \wedge A_{\gamma})$$

and

$$(\bigvee_{\alpha} A_{\alpha}) \wedge (\bigvee_{\beta} B_{\beta}) = \bigvee_{\alpha, \beta} (A_{\alpha} \wedge B_{\beta}).$$

These equations are to be interpreted in the sense that if the left side exists, then so does the right, and the two are equal.

If A and B are elements of a lattice with zero and unit and $A \wedge B = \Lambda$ and $A \vee B = \mathrm{V}$, then B is called a complement of A. Complements in a distributive lattice are unique if they exist, the unique complement of an element A being denoted by $\overline{A}$. A distributive lattice with distinct zero and unit that includes complements for all its elements is called a Boolean algebra.

2. Boolean Algebras

The definition of a Boolean algebra is based on the whole series of concepts and definitions set forth in the preceding section. It is possible, though, to translate the definition into a list of conditions that a set $\mathcal{A}$ of objects must satisfy in order to qualify as a Boolean algebra:

(1) Existence of a partial ordering: $\mathcal{A}$ must have an ordering that obeys the rules for partial orderings.

(2) Existence of a zero: $\mathcal{A}$ must have an element that minorizes all the other elements. (Such an element is necessarily unique and is denoted Λ.)

(3) Existence of a unit: $\mathcal{A}$ must have an element that majorizes all the other elements. (Such an element is necessarily unique and is denoted V.)

(4) Non-identity of the zero and unit: Λ and V must be distinct.

(Equivalently, $\mathcal{Q}$ must have at least two elements.)

(5) Existence of meets: For every pair of elements A and B in $\mathcal{Q}$, there is a greatest element among those that minorize them both. (This element is denoted by $A \wedge B$.)

(6) Existence of joins: For every pair of elements A and B in $\mathcal{Q}$, there is a least element among those that majorize them both. (This element is denoted $A \vee B$.)

(7) Distributivity: For any triplet of elements A, B and C in $\mathcal{Q}$, $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ and $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$.

(8) Existence of complements: For every element A there is an element B such that $A \wedge B = \perp$ and $A \vee B = \top$. (Such an element B is necessarily unique and is denoted $\overline{A}$.)

This list of conditions should enable us to decide whether our "Boolean algebras of propositions" and "Boolean algebras of probability masses" really pass muster to qualify as Boolean algebras in the mathematical sense.

Consider first a "Boolean algebra of propositions." I have been using this term to refer to any non-empty collection of propositions that includes the negation of each of its elements and the conjunction and disjunction of each pair of its elements. Such a collection does indeed satisfy the eight conditions listed above when it is partially ordered by implication -- i.e., when one proposition is said to minorize another if and only if it implies the other. The third rule for partial orderings then corresponds to the fact that propositions are held to be identical when they are logically equivalent. The zero and the unit are the impossible and sure propositions, respectively; the meet and join of two propositions are their conjunction and disjunction, respectively; and the complement of a proposition is its negation. The only one of the eight conditions that might cause any head-scratching is the requirement of distributivity, and careful thought will show it to be satisfied. So a "Boolean algebra of propositions" is indeed a Boolean algebra.

Since a Boolean algebra of propositions $\mathcal{A}$ contains the conjunction and disjunction of any pair of its elements, it also contains the conjunction and disjunction of any finite number $A_1, \ldots, A_n$ of its elements -- and of course the conjunction of the elements $A_1, \ldots, A_n$ will be their meet in $\mathcal{A}$ and their disjunction will be their join in $\mathcal{A}$. It should be noted, however, that $\mathcal{A}$ need not contain propositions corresponding to the logical conjunction or disjunction of any given infinite collection of its elements. If $\mathcal{A}$ does contain a proposition corresponding to the conjunction, say, of an infinite collection $\{A_\gamma\}_{\gamma\in\Gamma}$ of its elements, then that proposition would be the meet of the collection $\{A_\gamma\}_{\gamma\in\Gamma}$. But if $\mathcal{A}$ does not contain such a proposition, then the collection might not even have a meet -- and if it does have a meet, that meet might not be the conjunction of the elements $\{A_\gamma\}_{\gamma\in\Gamma}$. In short, finite meets and joins can always be interpreted as conjunctions and disjunctions, respectively, but infinite ones cannot always be.

How about "Boolean algebras of probability masses"? Do they qualify as Boolean algebras in the mathematical sense? As it stands now, our notion of a Boolean algebra of probability masses is based merely on the intuitive idea that probability masses are pieces of an idealized substanced called our "probability" -- an idealized substance that may not even consist of points. But it is evident that this intuitive idea readily fits with the eight conditions for Boolean algebras. The partial ordering is provided by setting $A \leq B$ whenever the probability mass A is part of the larger probability mass B. The unit, of course, is the entire probability mass. The existence of a zero is not so obvious: one might not at first contemplate a single probability mass that is part of all the others. But it is possible to invent a "null" probability mass and make it part of all the others by convention. The meet and join of two probability masses correspond intuitively to their "intersection" and "union"; while the complement of a given probability mass consists of precisely what is left over. The distributive laws are also intuitively valid.

There are a great many relations that are always satisfied by meets, joins and complements in a Boolean algebra, and I have taken several of them for granted in my discussions of Boolean algebras of propositions and Boolean algebras of probability masses.

Notice, for example, that for any two elements A and B of a Boolean algebra, $B \leq A$ if and only if $B \wedge \overline{A} = \curlywedge$. For if $B \leq A$, then $B \wedge \overline{A} \leq A \wedge \overline{A} = \curlywedge$. And if $B \wedge \overline{A} = \curlywedge$, then

$$(B \wedge \overline{A}) \vee (B \wedge A) = \curlywedge \vee (B \wedge A) = B \wedge A.$$

But by the first distributive law, the left-hand side of this equation is equal to $B \wedge (A \vee \overline{A}) = B \wedge \Upsilon = B$. So $B = B \wedge A$, and hence $B \leq A$. If $A \wedge B = \curlywedge$, then A and B are said to be <u>disjoint</u>; hence the preceding fact can be expressed by saying that $B \leq A$ if and only if B and $\overline{A}$ are disjoint. The quantity $B \wedge \overline{A}$ is often written as B-A.

If A, B, C are elements of a Boolean algebra, A and B are disjoint and $C = A \vee B$, then the expression "$A \vee B$" is called a <u>disjoint partition</u>

of C. Notice that for any two elements A, B in a Boolean algebra, $(A \wedge B) \vee (A - B)$ is a disjoint partition of A. Notice also that if $A \vee B$ is a disjoint partition of C and $A = C$, then $B = \Lambda$.

For any pair of elements A and B in a Boolean algebra,

$$\overline{A \vee B} = \overline{A} \wedge \overline{B} \qquad \text{and} \qquad \overline{A \wedge B} = \overline{A} \vee \overline{B}.$$

These identities, and the analogous ones for meets and joins of any finite number of elements, are known as de Morgan's laws.

Like a lattice, a Boolean algebra is called complete if it contains meets and joins for all its subsets, even infinite ones. Complete Boolean algebras obey the infinite version of De Morgan's laws, to wit:

$$\overline{\bigvee_{\gamma} A_{\gamma}} = \bigwedge_{\gamma} \overline{A}_{\gamma} \quad \text{and} \quad \overline{\bigwedge_{\gamma} A_{\gamma}} = \bigvee_{\gamma} \overline{A}_{\gamma}$$

We will sometimes be interested in the weaker condition of σ-completeness. A Boolean algebra is called σ-complete, of course, if it contains meets and joins for all countable collections of its elements.

3. The Mappings of Lattice Theory

Like any algebraic theory, the theory of lattices and Boolean algebras gives a prominent role to mappings that preserve the structure of its objects. In this section, we will learn the names of some of these mappings.

The simplest requirement in this context is that a mapping should preserve the structure of a semi-lattice. If $\mathcal{A}$ and $\mathcal{B}$ are meet-semi-lattices, for example, then a mapping $\theta: \mathcal{A} \to \mathcal{B}$ that obeys

(1) $\theta(A_1 \wedge A_2) = \theta(A_1) \wedge \theta(A_2)$ for all A_1, A_2 in $\mathcal{A}$

is called a meet-morphism. Similarly, if $\mathcal{A}$ and $\mathcal{B}$ are join-semilattices and a mapping $\theta: \mathcal{A} \to \mathcal{B}$ obeys

$$(2)\ \theta(A_1 \vee A_2) = \theta(A_1) \vee \theta(A_2) \text{ for all } A_1,\ A_2 \text{ in } \mathcal{A},$$

then θ is called a join -morphism. We saw examples of meet-morphisms in the preceding chapter: an allocation of probability is a meet-morphism, while a constraint mapping or an allowment is a join -morphism.

Meet-morphisms and join-morphisms are both order-preserving, or isotone; in other words, they both necessarily obey the rule

$$(3)\ \text{If } A_1 \leq A_2, \text{ then } \theta(A_1) \leq \theta(A_2).$$

This can be proven for a meet-morphism, for example, by using the fact that $A_1 \wedge A_2 = A_1$ whenever $A_1 \leq A_2$, for one obtains $\theta(A_1) = \theta(A_1 \wedge A_2) = \theta(A_1) \wedge \theta(A_2)$, whence $\theta(A_1) \leq \theta(A_2)$ by the definition of meet.

If $\mathcal{A}$ and $\mathcal{B}$ are lattices, then a mapping $\theta: \mathcal{A} \to \mathcal{B}$ is called a lattice homomorphism if it obeys both (1) and (2); i.e., if it is both a meet-morphism and a join-morphism. Finally, if $\mathcal{A}$ and $\mathcal{B}$ are Boolean algebras, then a mapping $\theta: \mathcal{A} \to \mathcal{B}$ is called a Boolean homomorphism if it obeys (1), (2), and

$$(4)\quad \theta(\overline{A}) = \overline{\theta(A)} \text{ for all } A \in \mathcal{A}.$$

In other words, a Boolean homomorphism is a lattice homomorphism that preserves complements. It can easily be deduced from de Morgan's law that if a mapping between two Boolean algebras obeys (4) and one of (1) and (2), then it must also obey the other. Hence in order for a mapping between two Boolean algebras to be a Boolean homomorphism, it suffices either for it to preserve complements and meets or for it to preserve complements and joins.

It is easily seen that a Boolean homomorphism $\theta: \mathcal{A} \to \mathcal{B}$ also preserves the unit and the zero; i.e., it obeys

(5) $\theta(\perp_{\mathcal{A}}) = \perp_{\mathcal{B}}$,

and (6) $\theta(\top_{\mathcal{A}}) = \top_{\mathcal{B}}$.

To prove (5), for example, note that for any $A \in \mathcal{A}$, $\theta(\perp_{\mathcal{A}}) = \theta(A \wedge \overline{A}) = \theta(A) \wedge \theta(\overline{A}) = \theta(A) \wedge \overline{\theta(A)} = \perp_{\mathcal{B}}$.

A subset $\mathcal{A}_o$ of a Boolean algebra $\mathcal{A}$ is called a <u>subalgebra</u> of $\mathcal{A}$ if it satisfies the following conditions:

(i) $\perp_{\mathcal{A}}$ and $\top_{\mathcal{A}}$ are in $\mathcal{A}_o$.

(ii) $\overline{A} \in \mathcal{A}_o$ for all $A \in \mathcal{A}_o$.

(iii) $A_1 \wedge A_2$ and $A_1 \vee A_2$ are in $\mathcal{A}_o$ for all pairs A_1, A_2 in $\mathcal{A}_o$.

Obviously, a subalgebra of a Boolean algebra is a Boolean algebra in its own right, its partial ordering being that inherited from the larger Boolean algebra. It is evident from equations (1), (2), (4), (5) and (6) that if θ: $\mathcal{A} \to \mathcal{B}$ is a Boolean homomorphism, then the image $\theta(\mathcal{A})$ is a subalgebra of $\mathcal{B}$.

If a Boolean homomorphism θ: $\mathcal{A} \to \mathcal{B}$ is one-to-one and onto, then it is called an <u>isomorphism onto</u> $\mathcal{B}$; it is easily verified that the inverse θ^{-1}: $\mathcal{B} \to \mathcal{A}$ will then be an isomorphism onto $\mathcal{A}$. If a Boolean homomorphism θ: $\mathcal{A} \to \mathcal{B}$ is merely one-to-one, it is called an <u>isomorphism into</u> $\mathcal{B}$; in such a case θ': $\mathcal{A} \to \theta(\mathcal{A})$:$A \rightsquigarrow \theta(A)$ will be an isomorphism onto the image $\theta(\mathcal{A})$, considered as a Boolean algebra in its own right. An isomorphism into is sometimes called an <u>embedding</u>.

If an isomorphism onto exists between two Boolean algebras $\mathcal{A}$ and $\mathcal{B}$, then the two are said to be isomorphic. Such an isomorphism onto will necessarily preserve arbitrary meets and joins. For example, if $\{A_\gamma\}_{\gamma\in\Gamma}$ and A are elements of $\mathcal{A}$, $A = \wedge A_\gamma$ and θ: $\mathcal{A} \to \mathcal{B}$ is an isomorphism onto, then $\wedge\, \theta(A_\gamma)$ will exist in $\mathcal{B}$ and will be equal to $\theta(A)$. This will not necessarily be true, though, if θ is merely an isomorphism into.

If $\mathcal{A}$ and $\mathcal{B}$ are both complete Boolean algebras, then a Boolean homomorphism $\theta: \mathcal{A} \to \mathcal{B}$ is called <u>complete</u> if it preserves arbitrary meets and joins -- i.e., if

$$(7) \quad \theta(\wedge A_\gamma) = \wedge\, \theta(A_\gamma)$$

and

$$(8) \quad \theta(\vee A_\gamma) = \vee\, \theta(A_\gamma)$$

for all collections $\{A_\gamma\}$ of elements of $\mathcal{A}$.

A subalgebra $\mathcal{A}_0$ of a complete Boolean algebra $\mathcal{A}$ is said to be a <u>complete subalgebra</u> if it includes meets and joins for arbitrary collections of its elements. A complete subalgebra is obviously a complete Boolean algebra. The image of a complete Boolean homomorphism is a complete subalgebra.

Similar statements can be made for σ-completeness: a subalgebra of a σ-complete Boolean algebra is called <u>σ-complete</u> if it is closed under countable meets and joins; a Boolean homomorphism between two σ-complete Boolean algebras is called <u>σ-complete</u> if it preserves countable meets and joins; and the image of a σ-complete Boolean homomorphism is a σ-complete subalgebra.

4. Filters and Ideals in Boolean Algebras

Filters and ideals are subsets of Boolean algebras that have certain closure properties. They play an important role in the general theory of Boolean algebras, and they will play an equally important role in our theory. They are so closely related that in a certain sense it would suffice to study only the one or the other, but it is more satisfying to learn about them both together.

A filter in a Boolean algebra $\mathcal{A}$ is a subset F of $\mathcal{A}$ that satisfies

(a) If $A \in F$ and $A \leq B$, then $B \in F$.

(b) If $A \in F$ and $B \in F$, then $A \wedge B \in F$.

(c) $\mathcal{V} \in F$.

Notice that (c) assures that a filter cannot be empty. An ideal in a Boolean algebra $\mathcal{A}$ is a subset I of $\mathcal{A}$ that satisfies

(a) If $A \in I$ and $B \leq A$, then $B \in I$.

(b) If $A \in I$ and $B \in I$, then $A \vee B \in I$.

(c) $\mathcal{\Lambda} \in I$.

Actually, we already encountered filters and ideals in Chapter 2. Indeed, a glance at the definition of a constraint relation is that chapter will reveal that the collection of all the propositions to which a given probability mass is constrained is a filter, while the collection of all the probability masses constrained to a given proposition is an ideal.

If A is any element of a Boolean algebra $\mathcal{A}$, then the subset $\{A' | A' \in \mathcal{A}, A \leq A'\}$ of $\mathcal{A}$ is a filter, while the subset $\{A' | A' \in \mathcal{A}, A' \leq A\}$ is an ideal. A filter or ideal of this form is called principal. It can easily be shown that any ideal or filter in a finite Boolean algebra must be principal. Suppose, for example, that F is a filter in a finite Boolean algebra $\mathcal{A}$. Let $A_1, \ldots, A_k$ be the elements of F. Then it follows from (b) in the definition of filter that $\bigwedge_{i=1}^{k} A_i \in F$. But $\bigwedge_{i=1}^{k} A_i \leq A_i$ for all i, and by (a) in the definition of filter, if $\bigwedge_{i=1}^{k} A_i \leq A$ for some $A \in \mathcal{A}$, then $A \in F$. Hence $F = \{A | A \in \mathcal{A}, \bigwedge_{i=1}^{k} A_i \leq A\}$.

The only subset of a Boolean algebra $\mathcal{A}$ that is both an ideal and a filter is $\mathcal{A}$ itself. An ideal or filter which is not equal to $\mathcal{A}$ is called a proper ideal or filter. It is evident that an ideal in $\mathcal{A}$ is proper if and only if it does not contain $\mathcal{V}$, while a filter in $\mathcal{A}$ is proper if and only if it does not contain Λ.

A filter F in a Boolean algebra $\mathcal{a}$ is called an <u>ultrafilter</u> if (i) F is proper and (ii) there is no other proper filter F' in $\mathcal{a}$ such that $F \neq F'$ and $F \subset F'$.

<u>Theorem</u>. A filter F in a Boolean algebra $\mathcal{a}$ is an ultrafilter if and only if for every element $A \varepsilon \mathcal{a}$ exactly one of the pair A, $\overline{A}$ is in F.

<u>Proof</u>: (i) Suppose that for each $A \varepsilon \mathcal{a}$, the filter F contains exactly one of the pair A, $\overline{A}$. Then $V \varepsilon F$ and $\overline{V} = \Lambda \notin F$, so F is proper. and if F' is a filter such that $F \neq F'$ and $F \subset F'$, there must be an element $A \varepsilon F'$ such that $A \notin F$. So $\overline{A}$ will be in F, whence $\overline{A} \varepsilon F'$ and $\overline{A} \wedge A = \Lambda \varepsilon F'$. Hence F' will not be proper. So F is an ultrafilter.

(ii) Now let us suppose that for some $A \varepsilon \mathcal{a}$, F does <u>not</u> contain exactly one of the pairs A, $\overline{A}$ and deduce that F is not an ultrafilter. We must consider the case where F contains both A and $\overline{A}$, and the case where it contains neither. If it contains both, then it would contain $A \wedge \overline{A} = \Lambda$ and hence would not be proper. If it contains neither, on the other hand, then the filter $F' = \{A' \mid A \wedge B \leq A' \text{ for some } B \varepsilon F\}$ satisfies $F \neq F'$ and $F \subset F'$, for F' contains both A and F. Furthermore, F' is proper. For if $\Lambda \varepsilon F$, then there exists some $B \varepsilon F$ such that $A \wedge B = \Lambda$, or $B \leq \overline{A}$, but this would contradict the assumption that $\overline{A} \notin F$. So F is contained in a larger proper filter and hence is not an ultrafilter. ▨

The notions of completeness can also be applied to filters and ideals. For example, an ideal in a σ-complete Boolean algebra is called a <u>σ-ideal</u> if it contains $\vee A_\gamma$ whenever it contains each element of a countable collection

$\{A_\gamma\}_{\gamma\in\Gamma}$. Similarly, an ideal in a complete Boolean algebra is called a complete ideal if it contains $\vee A_\gamma$ whenever it contains each element of an arbitrary collection $\{A_\gamma\}_{\gamma\in\Gamma}$. It is easily seen that an ideal in a complete Boolean algebra is complete if and only if it is principal.

5. Zorn's Lemma

In this section, I will state Zorn's lemma and us it to deduce some useful facts about Boolean algebras. Being equivalent to the principle of transfinite induction, Zorn's lemma is somewhat controversial among students of the foundations of mathematics, but it is generally accepted as a working tool. A proof of Zorn's lemma can be found on pp. 62-65 of Halmos' Naive Set Theory.

In order to state Zorn's lemma, we need the notions of a chain and of a maximal element in a partially ordered set. A maximal element in a partially ordered set is an element which is not a subelement of any other element. A unit in a partially ordered set is necessarily maximal, but a maximal element need not be a unit. A chain in a partially ordered set is a non-empty subset, any two elements A, B of which satisfy either $A \leq B$ or $B \leq A$.

Zorn's Lemma. If every chain in a partially ordered set has an upper bound, then that partially ordred set has at least one maximal element.

The two following theorems seem to require the use of Zorn's lemma in their proof.

Theorem. If F is a proper filter in a Boolean algebra $\mathcal{A}$, then F is contained in some ultrafilter in $\mathcal{A}$.

Proof: Let $\mathcal{S} = \{F' | F'$ is a proper filter in $\mathcal{A}$; $F \subset F'\}$, and let $\mathcal{S}$ be partially ordered by set inclusion. Notice that any maximal element of $\mathcal{S}$ is an ultrafilter. Hence we need only show that $\mathcal{S}$ has a maximal element. Let $\mathcal{K}$ be any chain in $\mathcal{S}$. Then it is easily seen that $\cup\mathcal{K}$ is a filter, and it is proper, for it does not contain Λ. Hence $\cup\mathcal{K}$ is in $\mathcal{S}$ and is an upper bound for the chain $\mathcal{K}$. Thus every chain in $\mathcal{S}$ has an upper bound, and by Zorn's lemma, $\mathcal{S}$ has a maximal element. ▨

Corollary. If A is a non-zero element of a Boolean algebra $\mathcal{A}$, then A is contained in some ultrafilter of $\mathcal{A}$.

Proof: A is contained in the proper filter $F = \{A' | A \leq A'\}$. ▨

Theorem. Suppose $\mathcal{A}$ is a Boolean algebra and $\mathcal{C} \subset \mathcal{A}$. Then there exists a subset $\mathcal{D} \subset \mathcal{A}$ such that (i) $\mathcal{D}$ is disjoint, (ii) for each $D \in \mathcal{D}$ there exists $C \in \mathcal{C}$ such that $D \leq C$, and (iii) $\mathcal{D}$ and $\mathcal{C}$ have the same set of upper bounds.

Proof: Set $\mathcal{S} = \{\mathcal{E} | \mathcal{E} \subset \mathcal{A}$; $\mathcal{E}$ is disjoint; and for each $E \in \mathcal{E}$ there exists $C \in \mathcal{C}$ such that $E \leq C\}$, and partially order $\mathcal{S}$ by set inclusion. If $\mathcal{S}_o$ is a chain in $\mathcal{S}$, then it is easily seen that $\cup\mathcal{S}_o$ is in $\mathcal{S}$; and $\cup\mathcal{S}_o$ will be an upper bound for $\mathcal{S}_o$ in $\mathcal{S}$. So every chain in $\mathcal{S}$ has an upper bound, and by Zorn's lemma $\mathcal{S}$ has at least one maximal element. Let $\mathcal{D}$ be such a maximal element of $\mathcal{S}$. Then it is evident that (i) $\mathcal{D}$ is disjoint, (ii) for each $D \in \mathcal{D}$ there exists an element $C \in \mathcal{C}$ such that $D \leq C$, and (iii) any upper bound of $\mathcal{C}$ is an upper bound for $\mathcal{D}$.

The proof will be complete if we can show that any upper bound A for $\mathcal{D}$ is an upper bound for $\mathcal{C}$. Consider any element $C \varepsilon \mathcal{C}$ and note that C-A will be disjoint from all the element s of $\mathcal{D}$. The set $\mathcal{D} \cup \{C-A\}$ will therefore be in $\mathcal{S}$. But $\mathcal{D}$ is already a maximal element of $\mathcal{S}$. Hence C-A must already be in $\mathcal{D}$, and this is possible only if $C-A = \Lambda$. It follows that $C \leq A$. Hence A is an upper bound for $\mathcal{C}$. ▨

6. Fields of Subsets

I used the notion of a field of subsets extensively in the preceding chapters, and I often switched back and forth between the notions of a field of subsets and the notion of a Boolean algebra of propositions. In particular, I often used three facts: (i) any field of subsets is a Boolean algebra under the partial ordering by set inclusion; (ii) any finite Boolean algebra is isomorphic to the field of all subsets of some finite set; (iii) any Boolean algebra, whether finite or not, is isomorphic to some field of subsets of some set. Now that we have a mathematical definition for the notion of a Boolean algebra, we can verify these three facts.

A non-empty collection $\mathcal{F}$ of subsets of a non-empty set $\mathcal{S}$ is called a <u>field of subsets</u> of $\mathcal{S}$ if whenever $\mathcal{F}$ contains two sets A and B, it also contains their union, their intersection, and their set-theoretic complements. In particular, it must contain some subset A of $\mathcal{S}$, the complement $\overline{A}$ of A, their intersection $A \cap \overline{A}$, which is the empty set ϕ, and their union $A \cup \overline{A}$, which is $\mathcal{S}$ itself. A given non-empty set $\mathcal{S}$ will have, of course, many different possible fields of subsets, ranging from the two-element field $\{\phi, \mathcal{S}\}$ to the field that includes all the subsets of $\mathcal{S}$. This latter field of subsets of $\mathcal{S}$ is called the power set of $\mathcal{S}$, and I will denote it by $\mathcal{P}(\mathcal{S})$.

It is easily verified that the binary relation "$\leq$" between a field of subsets $\mathcal{F}$ and itself defined by "$A \leq B$ if an only if $A \subset B$" is a partial ordering. Furthermore, $\mathcal{F}$ is a Boolean algebra under this partial ordering, the Boolean complement of an element being its set-theoretic complement, the meet of two elements being their intersection, the join of two elements being their union, the zero being ϕ, and the unit being $\mathcal{S}$. The meet and join of any finite collection of elements will also be their intersection and union, respectively; but the same is not necessarily true of infinite collections. If the intersection, say, of a given infinite collections of elements of $\mathcal{F}$ is in $\mathcal{F}$, then it will certainly be the meet of that collection; but otherwise the collection may have some other element of $\mathcal{F}$ as its meet, or may not even have a meet in $\mathcal{F}$.

The assertion that any Boolean algebra is isomorphic to a field of subsets is called the Stone Representation Theorem.

Theorem. Let $\mathcal{Q}$ be a Boolean algebra, let $\mathcal{S}$ be the set of ultrafilters in $\mathcal{Q}$, and for each $A \in \mathcal{Q}$, let $f(A)$ be the subset of $\mathcal{S}$ consisting of all the ultrafilters in $\mathcal{Q}$ that contain A, i.e., set $f(A) = \{F \mid F \in \mathcal{S}, A \in F\}$. Denote by $\mathcal{B}$ the collection of all subsets S of $\mathcal{S}$ such that $S = f(A)$ for some $A \in \mathcal{Q}$. Then $\mathcal{B}$ is a field of subsets of $\mathcal{S}$ and the mapping $f: \mathcal{Q} \to \mathcal{B} : A \leadsto f(A)$ is an isomorphism.

Proof: It is easily verified that $f(\Lambda_{\mathcal{Q}}) = \phi$ and $f(V_{\mathcal{Q}}) = \mathcal{S}$. In order to show that f preserves meets, we can use the fact that a filter in a

Boolean algebra contains both of a given pair of elements if and only if it contains their meet. Hence if A_1, $A_2 \in \mathcal{A}$, then

$$\begin{aligned} f(A_1)\cap f(A_2) &= \{F|F\in\mathcal{S},\ A_1\in F\}\cap\{F|F\in\mathcal{S},\ A_2\in F\} \\ &= \{F|F\in\mathcal{S},\ A_1\in F,\ A_2\in F\} \\ &= \{F|F\in\mathcal{S},\ A_1\wedge A_2\in F\} \\ &= f(A_1\wedge A_2). \end{aligned}$$

In order to show that f also preserves complements, it is necessary to use the fact that the filters in $\mathcal{S}$ are ultrafilters. This means that given any $A\in\mathcal{A}$, a filter F in $\mathcal{S}$ contains exactly one of the pair A and $\overline{A}$. Hence

$$\begin{aligned} \overline{f(A)} &= \overline{\{F|F\in\mathcal{S},\ A\in F\}} = \{F|F\in\mathcal{S},\ A\notin F\} \\ &= \{F|F\in\mathcal{S},\ \overline{A}\in F\} = f(\overline{A}) . \end{aligned}$$

It follows easily by de Morgan's laws that f also preserves joins. For if A_1, $A_2\in\mathcal{A}$, then

$$\begin{aligned} f(A_1\vee A_2) &= f(\overline{\overline{A}_1\wedge\overline{A}_2}) = \overline{f(\overline{A}_1\wedge\overline{A}_2)} = \overline{f(\overline{A}_1)\cap f(\overline{A}_2)} = \overline{\overline{f(A_1)}\cap\overline{f(A_2)}} \\ &= f(A_1)\cup f(A_2). \end{aligned}$$

These formulae prove in particular that $\mathcal{B}$ is a field. For if S is in $\mathcal{B}$, then there is an element $A\in\mathcal{A}$ such that $S = f(A)$ and hence $\overline{S} = f(\overline{A})$ is also in $\mathcal{B}$. And if S_1, $S_2\in\mathcal{B}$, then there exist A_1, $A_2\in\mathcal{A}$ such that $S_1 = f(A_1)$ and $S_2 = f(A_2)$, so that $S_1\cup S_2 = f(A_1\vee A_2)$ and $S_1\cap S_2 = f(A_1\wedge A_2)$ are also in $\mathcal{B}$.

Since B is a field and therefore a Boolean algebra, and since f preserves everything in sight, f is a Boolean homorphism. By the definition of $\mathcal{B}$, f is onto, hence it only remains to show that f is one-to-one.

In order to show that f is one-to-one, it is necessary to consider arbitrary elements A_1, $A_2\in\mathcal{A}$ such that $A_1\neq A_2$ and prove that $f(A_1) \neq f(A_2)$. In other words, one must show that there is some ultrafilter in $\mathcal{S}$ that contains exactly one of the pair A_1, A_2. But since $A_1 \neq A_2$, at least one of the relations $A_1 \leq A_2$ and $A_2 \leq A_1$ does not hold. We can assume that $A_1 \leq A_2$ does not hold. In that case, $A_1 \wedge \overline{A}_2 \neq \Lambda$. Hence, by the theorem proven in section 5, there must be at least one ultrafilter in $\mathcal{A}$ that contains $A_1 \wedge \overline{A}_2$. If F is such an ultrafilter, then F contains A_1, for $A_1 \wedge A_2 \leq A_1$. But F cannot contain A_2, for it contains $\overline{A}_2$. So F contains exactly one of the pair A_1, A_2. ▨

The set $\mathcal{S}$ is often called the Stone space of the Boolean algebra $\mathcal{A}$. Notice that the isomorphism f does map all finite meets and joins into the corresponding finite intersections and unions. It need not, however, take infinite meets and joins into the corresponding infinite set-theoretic intersections and unions.

The construction used in the Stone Representation Theorem can also be used to prove that a finite Boolean algebra is isomorphic to the field of all subsets of some set.

Theorem. Let $\mathcal{A}$ be a finite Boolean algebra and let $\mathcal{S}$ and $\mathcal{B}$ be as in the preceding theorem. Then $\mathcal{B}$ is the field of all subsets of $\mathcal{S}$.

Proof: Let F be an element of $\mathcal{S}$. Then F is an ultrafilter in $\mathcal{A}$. Since $\mathcal{A}$ is finite, F must be a principal filter; in other words, there must be a unique $A \in \mathcal{A}$ such that $F = \{A' \mid A \subset A'\}$. Since F is an ultrafilter, there cannot be any non-zero element B of $\mathcal{A}$ satisfying $B \subset A$, $B \neq A$. For if there were such an element, then the proper filter $\{A' \mid B \subset A'\}$ would properly contain F. It follows that F is the is the only proper filter containing A; in particular, it is the only ultrafilter containing A, and hence $f(A) = \{F\}$, and $\{F\} \in \mathcal{B}$.

Since we took F to be an arbitrary element of $\mathcal{S}$, it follows that every one-element subset of $\mathcal{S}$ is in $\mathcal{B}$. Since $\mathcal{S}$ is finite, it follows that all subsets of $\mathcal{S}$ are in $\mathcal{B}$.

Notice that $\mathcal{S}$ is in a one-to-one correspondence with the set of all non-zero elements of $\mathcal{A}$ that are not majorized by any other non-zero elements. These elements were called the atomic elements of $\mathcal{A}$ in our earlier discussions. ▨

It should also be noted that when $\mathcal{A}$ is finite the existence of an ultrafilter containing any given proper filter can be proven by induction, so that the preceding theorem, unlike the Stone Representation theorem, does not really depend upon Zorn's lemma.

A field of subsets is called a σ-field if it includes the intersection and the union of any countable collection of its elements. Such intersections and unions will of course be the meets and joins for such collections, so a σ-field will be a σ-complete Boolean algebra. Actually, the inclusion of either all such intersections or of all such unions is sufficient to imply the inclusion of the other.

7. Closure Properties

A property of subsets of a set $\mathcal{S}$ is called a closure property if (i) $\mathcal{S}$ has a property, and (ii) any intersection of subsets having the given property itself has the property. Suppose that "being an X" is a closure property for subsets of a set $\mathcal{S}$.

Then if C is any given subset of $\mathcal{S}$, the collection of all X's containing C is not empty, for $\mathcal{S}$ itself is an X that contains C. The intersection of all the X's containing C is also an X containing C -- in fact it is the least X containing C, in the sense that it is contained in any other X containing C. Hence whenever "being an X" is a closure property for subsets of $\mathcal{S}$ and $C \subset \mathcal{S}$, one may speak of the smallest X containing C, or of the X generated by C.

There are several closure properties that will interest us in this essay. First, the property of "being an ideal" is a closure property for subsets of a Boolean algebra $\mathcal{Q}$. Hence we may speak of the smallest ideal containing any given subset of $\mathcal{Q}$, or of the ideal generated by that subset. In fact, the ideal generated by a non-empty subset $\mathcal{C} \subset \mathcal{Q}$ is given by $\{A | A \in \mathcal{Q}$ and $A \leq A_1 \vee \ldots \vee A_n$ for some finite collection $A_1, \ldots, A_n$ of elements of $\mathcal{C}\}$. In particular, the ideal generated by the singleton $\{A\}$ is given by $\{A' | A' \in \mathcal{Q}, A' \leq A\}$.

Secondly, the property of being a filter is also a closure property for subsets of a Boolean algebra. The filter generated by a non-empty subset $\mathcal{C}$ of a Boolean algebra $\mathcal{Q}$ is given by $\{A | A \in \mathcal{Q}$ and $A_1 \wedge \ldots \wedge A_n \leq A$ for some finite collection $A_1, \ldots, A_n$ of elements of $\mathcal{C}\}$.

Thirdly, the property of being a subalgebra is a closure property for subsets of a Boolean algebra. The subalgebra generated by a non-empty subset $\mathcal{C}$ of a Boolean algebra $\mathcal{Q}$ consists precisely of all those elements A of $\mathcal{Q}$ of the form

$$A = (A_{1,1} \wedge \ldots \wedge A_{1,r_1}) \vee (A_{2,1} \wedge \ldots \wedge A_{2,r_s}) \vee \ldots \vee (A_{s,1} \wedge \ldots \wedge A_{s,r_s}),$$

where for each m, n either $A_{m,n} \in \mathcal{C}$ or $\overline{A}_{m,n} \in \mathcal{C}$. Similarly, the property of being a complete subalgebra is a closure property for subsets of a complete Boolean algebra.

Finally, the property of being a field of subsets of the set $\mathcal{S}$ is a closure property for subsets of the power set $\mathcal{P}(\mathcal{S})$. Hence we may speak of the field of subsets of $\mathcal{S}$ generated by any collection of subsets of $\mathcal{S}$. The property of being a σ-field of subsets of $\mathcal{S}$ will also be a closure property for subsets of the power set $\mathcal{P}(\mathcal{S})$.

8. Quotients of Boolean Algebras

This section is devoted to the notion of dividing a Boolean algebra by an ideal.

If A and B are two elements in a Boolean algebra $\mathcal{A}$, then the element $(A - B) \vee (B - A) = (A \vee B) - (A \wedge B)$ is called the symmetric difference of A and B and is denoted $A \Delta B$. Notice that if A, B, and C are elements of $\mathcal{A}$, then

$$\begin{aligned} A \Delta C &= (A \Delta C) \wedge (B \vee \overline{B}) \\ &= (A \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge B \wedge C) \vee (A \wedge \overline{B} \wedge \overline{C}) \vee (\overline{A} \wedge \overline{B} \wedge C) \\ &\leq (B \wedge \overline{C}) \vee (\overline{A} \wedge B) \vee (A \wedge \overline{B}) \vee (\overline{B} \wedge C) \\ &= (A \Delta B) \vee (B \Delta C). \end{aligned}$$

Suppose we fix a proper ideal I in $\mathcal{A}$ and write "$A \approx B$" whenever A and B are in $\mathcal{A}$ and $A \Delta B \in I$. Then the relation "$\approx$" is a equivalence relation for elements of $\mathcal{A}$. In other words, it is reflexive, symmetric and transitive:

(i) If $A \in \mathcal{A}$, then $A \Delta A = \perp \in I$ and $A \approx A$.

(ii) If $A \approx B$, then $B \approx A$.

(iii) If $A \approx B$ and $B \approx C$, then $A \Delta C \leq (A \Delta B) \vee (B \Delta C)$; so $A \Delta C \in I$ and $A \approx C$.

The set of equivalence classes induced by this equivalence relation is called the quotient of $\mathcal{Q}$ by I and denoted $\mathcal{Q}/I$. In other words,

$$\mathcal{Q}/I = \left\{ \{B \mid B \in \mathcal{Q} \text{ and } B \approx A\} \,\middle|\, A \in \mathcal{Q} \right\}.$$

It is convenient to denote by [A] the equivalence class

$$\{B \mid B \in \mathcal{Q} \text{ and } B \approx A\}.$$

A binary relation "$\leq$" between $\mathcal{Q}/I$ and itself can be defined by setting $S_1 \leq S_2$ whenever S_1, $S_2 \in \mathcal{Q}/I$ and there are elements $A_1 \in S_1$ and $A_2 \in S_2$ such that $A_1 \leq A_2$. It is straightforward but tedious to verify that this binary relation is a partial ordering and that it makes $\mathcal{Q}/I$ into a Boolean algebra.

Furthermore, the mapping

$$f: \mathcal{Q} \to \mathcal{Q}/I : A \rightsquigarrow [A]$$

is a Boolean homomorphism. It is onto, of course, and it is called the canonical homomorphism of $\mathcal{Q}$ onto $\mathcal{Q}/I$. Notice in particular that the zero of $\mathcal{Q}/I$ is $I = [\Lambda_{\mathcal{Q}}]$, while the unit of $\mathcal{Q}/I$ is $[V_{\mathcal{Q}}]$.

When $\mathcal{Q}$ is a Boolean algebra of propositions, the quotient $\mathcal{Q}/I$ has an epistemic interpretation. Suppose, indeed, that one first contemplates $\mathcal{Q}$ without knowing whether any given propositions in it are true or false, except for V and Λ, which one knows to be true and false, respectively. Suppose further that one then learns that all the propositions in a given proper ideal I are also false. When this happens, one can regard all the propositions in I as "logically equivalent" to the impossible proposition . And we can say even more. If A, B $\in \mathcal{Q}$, then one of the pair A, B can be false and the other true only if $A \Delta B$ is true. Hence if $A \Delta B$ is in I, the knowledge that all the propositions in I are false tells one that A is true if and only if B is true -- i.e., A and B become logically equivalent. In general, then, the knowledge that all the propositions in I are false leads one to regard all the propositions in any given equivalence class as logically equivalent. Identifying propositions that are now seen as equivalent then amounts to replacing the Boolean algebra $\mathcal{Q}$ by the Boolean algebra $\mathcal{Q}/I$.

Of course, one might learn that the set J of propositions is false, where $J \subset \mathcal{Q}$ but J is not an ideal. In this case, the falsity of the propositions in J would imply the falsity of all the propositions that imply some proposition in J or the disjunction of some finite collection of propositions in J. But this latter collection of propositions, $I = \{A | A \leq A_1 \vee \ldots \vee A_n$ for some finite collection $A_1, \ldots, A_n$ of elements of $J\}$, is the ideal generated by J. Hence the total collection of propositions learned to be false will be an ideal, and the preceding analysis will apply. An important special case occurs when J is a singleton $\{A\}$; in this case, I is the principal ideal generated by A.

We will often be interested, of course, in the case where $\mathcal{Q} = \mathcal{P}(\mathcal{S})$ for some set $\mathcal{S}$, and the propositions all concern the true value of some parameter that takes values in $\mathcal{S}$. In this case, the ideal I usually arises by the discovery that the true value is in some subset $\mathcal{S}_0 \subset \mathcal{S}$. The ideal I of propositions learned to be false by virtue of such a discovery is precisely the principal ideal generated by $\overline{\mathcal{S}}_0$, and $\mathcal{Q}/I$ will be isomorphic to $\mathcal{P}(\mathcal{S}_0)$.

In Chapters 4 and 7, we will study another application of the notion of a quotient of a Boolean algebra by an ideal, this time to the case of a Boolean algebra of probability masses.

I will conclude this section with two theorems, one with a proof and the other without.

Theorem. Suppose $\mathcal{A}$ is a σ-complete Boolean algebra and I is a proper σ-ideal of $\mathcal{A}$. Then $\mathcal{A}/I$ is σ-complete, and the canonical Boolean homomorphism

$$f: \mathcal{A} \to \mathcal{A}/I : A \rightsquigarrow [A]$$

is σ-complete.

Proof: The σ-completeness of both $\mathcal{A}/I$ and f follows from the following fact: If $A_1, A_2, \ldots$ is a sequence of elements of $\mathcal{A}$, then $[A_1], [A_2], \ldots$ has a join in $\mathcal{A}/I$, and in fact $\vee[A_i] = [\vee A_i]$. To prove this fact, note first that by the monotonicity of the Boolean homomorphism f, $[A_i] \leq [\vee A_i]$ for all i. Hence we need only prove that if $[A_i] \leq [B]$ for all i, then $[\vee A_i] \leq [B]$. But since the Boolean homomorphism f preserves differences, $[A_i] \leq [B]$ means that $\Lambda = [A_i] - [B] = [A_i - B]$, whence $A_i - B \in I$ for each i. But I is a σ-ideal, so $\vee(A_i - B) = (\vee A_i - B) \in I$. Hence $\Lambda = f(\vee A_i - B)$ $= [\vee A_i - B] = [\vee A_i] - [B]$, or $[\vee A_i] \leq [B]$. ▨

The Loomis-Sikorski Representation Theorem. For every σ-complete Boolean algebra $\mathcal{A}$ there exists a σ-field of sets $\mathcal{F}$ and a σ-ideal I of $\mathcal{F}$ such that $\mathcal{A}$ is isomorphic to $\mathcal{F}/I$.

Proofs of this theorem can be found in Sikorski (p. 117), Birkhoff (p. 255), or in Halmos' Lectures (p. 102).

9. Independent Sums of Boolean Algebras

Suppose $A_1, \ldots, A_n$ are subalgebras of a Boolean algebra $\mathcal{A}$. Then these n subalgebras are said to be <u>independent</u> if

$$A_1 \wedge \ldots \wedge A_n \neq \Lambda$$

whenever $A_i \varepsilon \mathcal{A}_i$ and $A_i \neq \Lambda$ for each i, i = 1, ..., n. When $\mathcal{A}$ is a Boolean algebra of propositions, this notion corresponds to the intuitive idea of logical independence. Indeed, two subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ will be independent if and only if a non-sure proposition in one of them is never implied by a non-impossible proposition in the other. And more generally, n subalgebras $\mathcal{A}_1, \ldots, \mathcal{A}_n$ are independent if and only if a non-sure proposition in one of them is never implied by the conjunction of non-impossible propositions from the others.

Some of the implications of independence are developed by the following propositions.

<u>Theorem</u>. Suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent subalgebras of a Boolean algebra $\mathcal{A}$. Suppose $A_1, A_1' \varepsilon \mathcal{A}_1, A_2, A_2' \varepsilon \mathcal{A}_2$, and $\Lambda \neq A_1' \wedge A_2' \leq A_1 \wedge A_2$. Then $A_1' \leq A_1$ and $A_2' \leq A_2$.

<u>Proof:</u>

$$A_1' \wedge A_2' = [(A_1' \wedge A_1) \vee (A_1' - A_1)] \wedge A_2'$$
$$= [(A_1' \wedge A_1) \wedge A_2'] \vee [(A_1' - A_1) \wedge A_2']$$

is a disjoint partition. But $A_1' \wedge A_2' = (A_1' \wedge A_2') \wedge A_1 = (A_1' \wedge A_1) \wedge A_2'$. So $(A_1' - A_1) \wedge A_2' = \Lambda$. Hence, by independence, $A_1' - A_1 = \Lambda$. This means $A_1' \leq A_1$. Similarly, $A_2' \leq A_2$. ▨

Corollary. Suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent subalgebras of a Boolean algebra $\mathcal{A}$. Suppose $A \in \mathcal{A}$, $A \neq \Lambda$, and $A = A_1' \wedge A_2' = A_1 \wedge A_2$, where $A_1, A_1' \in \mathcal{A}_1$, and $A_2, A_2' \in \mathcal{A}_2$. Then $A_1 = A_1'$ and $A_2 = A_2'$.

Corollary. Suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent subalgebras of a Boolean algebra $\mathcal{A}$, that $A_1, A_1' \in \mathcal{A}$, that $A_2, A_2' \in \mathcal{A}_2$, and that $\Lambda \neq A_1' \wedge A_2' < A_1 \wedge A_2$. Then $A_1' \leq A_1$, $A_2' \leq A_2$ and either $A_1 < A_1'$ or $A_2 < A_2'$.

Theorem. Suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent subalgebras of $\mathcal{A}$ and generate $\mathcal{A}$. Suppose $A_o \in \mathcal{A}$, $A \in \mathcal{A}_1$, $B \in \mathcal{A}_2$, and $\Lambda \neq A_o < A \wedge B$. Then there exists an integer $s \geq 1$ and elements $A_1, \ldots, A_s \in \mathcal{A}_1$ and elements $B_1, \ldots, B_s \in \mathcal{A}_2$ such that $A_i \leq A$ and $B_i \leq B$ for $i = 1, \ldots, s$, and

$$A_o = (A_1 \wedge B_1) \vee \ldots \vee (A_s \wedge B_s) \qquad (1)$$

Proof: Since $\mathcal{A}$ is generated by $\mathcal{A}_1 \cup \mathcal{A}_2$, the element A_o must, by section 7, be of the form

$$A_o = (A_{1,1} \wedge \ldots \wedge A_{1,r_1}) \vee (A_{2,1} \wedge \ldots \wedge A_{2,r_2}) \vee \ldots \vee$$

$$(A_{s,1} \wedge \ldots \wedge A_{s,r_s}),$$

where for each m, n either $A_{m,n} \in \mathcal{A}_1 \cup \mathcal{A}_2$ or $\overline{A}_{m,n} \in \mathcal{A}_1 \cup \mathcal{A}_2$. And since $\mathcal{A}_1$ and $\mathcal{A}_2$ are subalgebras, this means that A must be of the form (1). Since we may assume that the $A_i \wedge B_i$ are non-zero, the fact that the $A_i \leq A$ and the $B_i \leq B$ follows from the preceding theorem. ▨

Theorem. Suppose $A_1 \in \mathcal{Q}_1$, $A_1 \neq \Lambda$, and $A_2, A_2' \in \mathcal{Q}_2$, where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are independent subalgebras of $\mathcal{Q}$. And suppose that $A_1 \wedge A_2 \leq A_2'$. Then $A_2 \leq A_2'$.

Proof: If $A_1 \wedge A_2 \leq A_2'$, then $A_1 \wedge A_2 \wedge \overline{A_2'} = \Lambda$, whence $A_2 \wedge \overline{A_2'} = \Lambda$, or $A_2 \leq A_2'$.

Theorem. Suppose $A_1, A_1' \in \mathcal{Q}_1$ and $A_2, A_2' \in \mathcal{Q}_2$, where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are independent subalgebras of $\mathcal{Q}$. And suppose that $A_1 \wedge A_2 \leq A_1' \vee A_2'$. Then $A_1 \leq A_1'$ or $A_2 \leq A_2'$.

Proof: $(A_1 \wedge A_2) \wedge \overline{A_1'} \leq (A_1' \vee A_2') \wedge \overline{A_1'} \leq A_2'$. Hence $(A_1 \wedge \overline{A_1'}) \wedge A_2 \leq A_2'$. So by the preceding theorem, either $A_1 \wedge A_1' = \Lambda$ and $A_1 \leq A_1'$, or $A_2 \leq A_2'$.

Now suppose we have a collection $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ of Boolean algebras and that we conceive of them in the first instance as having nothing to do with each other. Then we might still wish to think of them as independent subalgebras of some larger Boolean algebra. If, for example, they are Boolean algebras of propositions, each dealing with a different subject, then we might wish to embed them in an overall Boolean algebra of propositions which would also contain propositions of the form (1) -- propositions dealing with more than one subject at a time.

Abstractly, what would it mean to embed the Boolean algebras $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ as independent subalgebras of a larger algebra $\mathfrak{A}$? Well, one would require a collection of isomorphisms $f_1, \ldots, f_n$ such that for each i, $i = 1, \ldots, n$, f_i is an isomorphism of $\mathfrak{A}_i$ into $\mathfrak{A}$; and one would require that the images $f_1(\mathfrak{A}_1), \ldots, f_n(\mathfrak{A}_n)$ should be independent subalgebras of $\mathfrak{A}$.

Now we might carry out such an embedding and then find out that the algebra $\mathfrak{A}$ is larger than it needs to be. In other words, the subalgebra of $\mathfrak{A}$ generated by $f_1(\mathfrak{A}_1) \cup \ldots \cup f_n(\mathfrak{A}_n)$ might be a proper subalgebra of $\mathfrak{A}$. If this occurs, though, we can replace $\mathfrak{A}$ by that proper subalgebra and still have an embedding -- one which would now be "minimal". This leads us to the following definition:

Definition. Suppose $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{A}$ are Boolean algebras and that for each i, $i = 1, \ldots, n$, $f_i: \mathfrak{A}_i \to \mathfrak{A}$ is an isomorphism into. Suppose further that $f_1(\mathfrak{A}_1), \ldots, f_n(\mathfrak{A}_n)$ are independent subalgebras of $\mathfrak{A}$ and that $f_1(\mathfrak{A}_1) \cup \ldots \cup f_n(\mathfrak{A}_n)$ generates $\mathfrak{A}$. Then $(f_1, \ldots, f_n; \mathfrak{A})$ is called an independent sum of $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$.

As is turns out, an independent sum of $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ always exists. (See Sikorski, pp. 40-41.) Furthermore, all such independent sums are isomorphic, in the sense that for any two of them, say $(f_1, \ldots, f_n, \mathfrak{A})$ and $(f_1', \ldots, f_n', \mathfrak{A}')$ there is an isomorphism h of $\mathfrak{A}$ onto $\mathfrak{A}'$ such that $f_i' = h \circ f_i$ for each i, $i = 1, \ldots, n$. Hence the independent sum of a collection of Boolean algebras is essentially unique.

When the Boolean algebras are thought of as Boolean algebras of propositions this uniqueness is reassuring, for each element of the independent sum is given an intuitive interpretation by formula (1).

Often, of course, each of the Boolean algebras $\mathcal{A}_i$ is conceived of as a field of subsets of some set $\mathcal{S}_i$. In this case, the sum can be thought of as a field of subsets of the Cartesian product $\mathcal{S} = \mathcal{S}_1 \times \ldots \times \mathcal{S}_n$. Indeed, the isomorphisms f_i are defined by $f_i(A) = \mathcal{S}_1 \times \ldots \times \mathcal{S}_{i-1} \times A \times \mathcal{S}_{i+1} \times \ldots \mathcal{S}_n$, and the sum $\mathcal{A}$ is then the field of subsets of $\mathcal{S}$ generated by the collection $f_1(\mathcal{A}_1) \cup \ldots \cup f_n(\mathcal{A}_n)$.

In general, I will denote by $\mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n$ the independent sum of the collection $\mathcal{A}_1, \ldots, \mathcal{A}_n$. Properly speaking, the Boolean algebras $\mathcal{A}_1, \ldots, \mathcal{A}_n$ will only be isomorphic to independent subalgebras of $\mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n$. But I will often speak of them as if they actually were subalgebras of $\mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n$. This practice is often quite convenient and does not seem to cause confusion.